PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-142702
(43)Date of publication of application : 02.06.2005

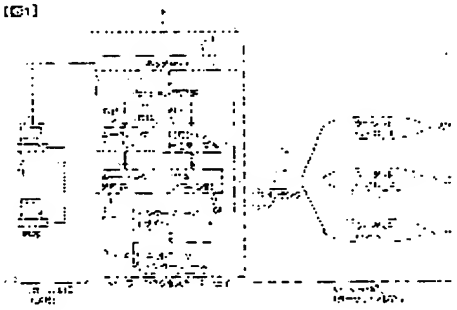
(51)Int.Cl. H04L 12/66
H04L 12/46
H04L 12/56

(21)Application number : 2003-375352
(22)Date of filing : 05.11.2003

(71)Applicant : NEC CORP
(72)Inventor : FUJITA NORITO
ISHIKAWA YUICHI
IWATA ATSUSHI

(54) NETWORK ACCESS GATEWAY, NETWORK ACCESS GATEWAY CONTROL METHOD, AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable each terminal in a LAN accommodated in the network access gateway to access an optional number of target networks (target VLAN) at the same time.
SOLUTION: When receiving an authentication request particularizing a target VLAN (e.g. target VLAN D1, D3) desirably accessed from a terminal A1 in the LAN, a terminal authentication section B11 in the network access gateway B1 authenticates whether or not the access to the target VLAN D1, D3 is possible. When accessible, a session management section B12 generates a virtual interface to an interface driver B17 so that the access from the terminal A1 to the target VLAN D1, D3 is possible and makes settings for transfer of packets transmitted from / received by the terminal A1 to a routing table B13 and further settings for transfer of a DNS query transmitted from the terminal A1 to a DNS query transfer table B15.



LEGAL STATUS

[Date of request for examination] 05.11.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-142702
(P2005-142702A)
(43)公開日　平成17年6月2日(2005.6.2)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/66	H04L 12/66	A	5K030
H04L 12/46	H04L 12/46	V	5K033
H04L 12/56	H04L 12/56	H	

審査請求 有　請求項の数 39　OL　（全 37 頁）

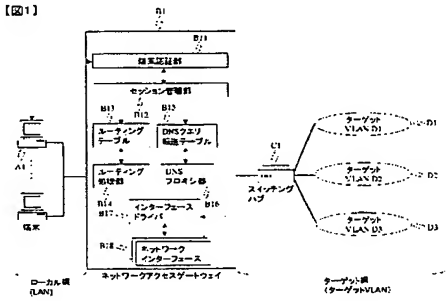
(21)出願番号　特願2003-375352 (P2003-375352)
(22)出願日　平成15年11月5日 (2003.11.5)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100088959
弁理士　境　廣巳
(72)発明者　藤田　範人
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　石川　雄一
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　岩田　淳
東京都港区芝五丁目７番１号　日本電気株式会社内

最終頁に続く

(54)【発明の名称】ネットワークアクセスゲートウェイ及びネットワークアクセスゲートウェイの制御方法並びにプログラム

(57)【要約】
【課題】ネットワークアクセスゲートウェイに収容されるLAN内の各端末が、それぞれ任意の数のターゲット網（ターゲットVLAN）に同時にアクセスできるようにする。
【解決手段】ネットワークアクセスゲートウェイB1内の端末認証部B11は、LAN内の端末A1からアクセスしたいターゲットVLAN（例えば、ターゲットVLAN D1, D3）を特定した認証要求が送られてくると、ターゲットVLAN D1, D3に対するアクセスが可能か否かを認証する。アクセス可能な場合、セッション管理部B12は、端末A1からターゲットVLAN D1, D3へのアクセスが可能になるように、インターフェースドライバB17に対して仮想インターフェースを作成すると共に、端末A1が送受信するパケットを転送するための設定をルーティングテーブルB13に対して行い、さらに端末A1が送信するDNSクエリを転送するための設定をDNSクエリ転送テーブルB15に対して行う。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイであって、
前記ノードごとに、１つまたは複数の前記ターゲット網へのアクセスのための環境設定を行えることを特徴とするネットワークアクセスゲートウェイ。
【請求項２】
前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする請求項１に記載のネットワークアクセスゲートウェイ。
【請求項３】
ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイであって、
複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証部と、
該端末認証部で認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理部とを備えること
を特徴とするネットワークアクセスゲートウェイ。
【請求項４】
前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする請求項３に記載のネットワークアクセスゲートウェイ。
【請求項５】
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、
前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第２のエントリが格納される名前解決クエリ転送テーブルとを備え、
前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記ルーティングテーブルに対して第１のエントリを作成し、前記名前解決クエリ転送テーブルに対して第２のエントリを作成すること
を特徴とする請求項３または４のいずれかに記載のネットワークアクセスゲートウェイ。
【請求項６】
前記名前解決クエリはＤＮＳクエリであり、前記名前解決クエリ転送テーブルはＤＮＳクエリ転送テーブルであること
を特徴とする請求項５に記載のネットワークアクセスゲートウェイ。
【請求項７】
前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うこと
を特徴とする請求項３乃至６のいずれかに記載のネットワークアクセスゲートウェイ。
【請求項８】
前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有す

る認証ＶＬＡＮスイッチに問い合わせることにより認証を行うこと
を特徴とする請求項３乃至６のいずれかに記載のネットワークアクセスゲートウェイ。
【請求項９】
前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得する設定クライアントを有すること
を特徴とする請求項３乃至８のいずれかに記載のネットワークアクセスゲートウェイ。
【請求項１０】
前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられること
を特徴とする請求項３乃至９のいずれかに記載のネットワークアクセスゲートウェイ。
【請求項１１】
複数の前記ターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求める機能を有するＩＰアドレス領域重複検出部を備えること
を特徴とする請求項３乃至１０のいずれかに記載のネットワークアクセスゲートウェイ。
【請求項１２】
前記セッション管理部は、
前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記ＩＰアドレス領域重複検出部を介して、前記複数のターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求め、
前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第３のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、
重複するＩＰアドレス領域を互いに重複しないＩＰアドレス領域にＩＰアドレス変換するように第１のエントリおよび第３のエントリを設定すること
を特徴とする請求項１１に記載のネットワークアクセスゲートウェイ。
【請求項１３】
前記名前解決クエリはＤＮＳクエリであり、前記名前解決応答はＤＮＳ応答であり、前記名前解決クエリ／応答転送テーブルはＤＮＳクエリ／応答転送テーブルであること
を特徴とする請求項１２に記載のネットワークアクセスゲートウェイ。
【請求項１４】
ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイの制御方法であって、
前記ノードごとに、１つまたは複数の前記ターゲット網へのアクセスのための環境設定を行うことを特徴とするネットワークアクセスゲートウェイの制御方法。
【請求項１５】
前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする請求項１４に記載のネットワークアクセスゲートウェイの制御方法。
【請求項１６】
ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイの制御方法であって、

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証ステップと、
該端末認証ステップで認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理ステップとを含むこと
を特徴とするネットワークアクセスゲートウェイの制御方法。
【請求項１７】
前記セッション管理ステップは、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成すること
を特徴とする請求項１６に記載のネットワークアクセスゲートウェイの制御方法。
【請求項１８】
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、
前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第２のエントリが格納される名前解決クエリ転送テーブルとを備え、
前記セッション管理ステップでは、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記ルーティングテーブルに対して第１のエントリを作成し、前記名前解決クエリ転送テーブルに対して第２のエントリを作成すること
を特徴とする請求項１６または１７のいずれかに記載のネットワークアクセスゲートウェイの制御方法。
【請求項１９】
前記名前解決クエリはＤＮＳクエリであり、前記名前解決クエリ転送テーブルはＤＮＳクエリ転送テーブルであること
を特徴とする請求項１８に記載のネットワークアクセスゲートウェイの制御方法。
【請求項２０】
前記端末認証ステップでは、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うこと
を特徴とする請求項１６乃至１９のいずれかに記載のネットワークアクセスゲートウェイの制御方法。
【請求項２１】
前記端末認証ステップでは、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証ＶＬＡＮスイッチに問い合わせることにより認証を行うこと
を特徴とする請求項１６乃至１９のいずれかに記載のネットワークアクセスゲートウェイの制御方法。
【請求項２２】
前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得するパラメータ取得ステップを含むこと
を特徴とする請求項１６乃至２１のいずれかに記載のネットワークアクセスゲートウェイの制御方法。
【請求項２３】
前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられること

を特徴とする請求項１６乃至２２のいずれかに記載のネットワークアクセスゲートウェイの制御方法。

【請求項２４】

複数の前記ターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求める機能を有するＩＰアドレス領域重複検出ステップを含むこと
を特徴とする請求項１６乃至２３のいずれかに記載のネットワークアクセスゲートウェイの制御方法。

【請求項２５】

前記セッション管理ステップでは、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記ＩＰアドレス領域重複検出ステップを介して、前記複数のターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第３のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するＩＰアドレス領域を互いに重複しないＩＰアドレス領域にＩＰアドレス変換するように第１のエントリおよび第３のエントリを設定すること
を特徴とする請求項２４に記載のネットワークアクセスゲートウェイの制御方法。

【請求項２６】

前記名前解決クエリはＤＮＳクエリであり、前記名前解決応答はＤＮＳ応答であり、前記名前解決クエリ／応答転送テーブルはＤＮＳクエリ／応答転送テーブルであること
を特徴とする請求項２５に記載のネットワークアクセスゲートウェイの制御方法。

【請求項２７】

コンピュータを、ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイとして機能させるためのプログラムであって、

前記コンピュータを、前記ノードごとに、１つまたは複数の前記ターゲット網へのアクセスのための環境設定を行えるネットワークアクセスゲートウェイとして機能させるためのプログラム。

【請求項２８】

前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする請求項２７に記載のプログラム。

【請求項２９】

コンピュータを、ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイとして機能させるためのプログラムであって、

前記コンピュータを、

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証部、

該端末認証部で認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理部として機能させるためのプログラム。

【請求項３０】

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための

環境設定として、
前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする請求項２９に記載のプログラム。
【請求項３１】
前記コンピュータが、
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、
前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第２のエントリが格納される名前解決クエリ転送テーブルとを備え、
前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記ルーティングテーブルに対して第１のエントリを作成し、前記名前解決クエリ転送テーブルに対して第２のエントリを作成すること
を特徴とする請求項２９または３０のいずれかに記載のプログラム。
【請求項３２】
前記名前解決クエリはＤＮＳクエリであり、前記名前解決クエリ転送テーブルはＤＮＳクエリ転送テーブルであること
を特徴とする請求項３１に記載のプログラム。
【請求項３３】
前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うこと
を特徴とする請求項２９乃至３２のいずれかに記載のプログラム。
【請求項３４】
前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証ＶＬＡＮスイッチに問い合わせることにより認証を行うこと
を特徴とする請求項２９乃至３２のいずれかに記載のプログラム。
【請求項３５】
前記コンピュータを、
前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得する設定クライアントとして機能させること
を特徴とする請求項２９乃至３４のいずれかに記載のプログラム。
【請求項３６】
前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられること
を特徴とする請求項２９乃至３５のいずれかに記載のプログラム。
【請求項３７】
前記コンピュータを、
複数の前記ターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求めるＩＰアドレス領域重複検出部として機能させること
を特徴とする請求項２９乃至３６のいずれかに記載のプログラム。
【請求項３８】
前記セッション管理部は、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記ＩＰアドレス領域重複検出部を介して、前記複数のターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第３のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するＩＰアドレス領域を互いに重複しないＩＰアドレス領域にＩＰアドレス変換するように第１のエントリおよび第３のエントリを設定すること

を特徴とする請求項３７に記載のプログラム。

【請求項３９】

前記名前解決クエリはＤＮＳクエリであり、前記名前解決応答はＤＮＳ応答であり、前記名前解決クエリ／応答転送テーブルはＤＮＳクエリ／応答転送テーブルであること

を特徴とする請求項３８に記載のプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワークアクセスゲートウェイに関し、特に、ＬＡＮ(Local Area Network)内のノードとＷＡＮ(Wide Area Network)との境界に設置され、ＬＡＮ内のノードをＷＡＮに接続させるネットワークアクセスゲートウェイに関する。

【背景技術】

【０００２】

従来からＬＡＮ内のノードとＷＡＮとの境界に設置され、ＬＡＮ内のノードをＷＡＮに接続させるためのネットワークアクセスゲートウェイとしては種々のものが知られている（例えば、特許文献１参照）。このようなネットワークアクセスゲートウェイの利用例としては、家庭やオフィスからインターネットや企業基幹網にアクセスするためのアクセスゲートウェイとしての利用が挙げられる。また他にも、網事業者における利用も考えられ、ホットスポット、マンション、オフィスビルディング等における加入者ノードの集線装置としての利用が挙げられる。網事業者における利用の場合は、加入者認証機能や課金機能など、家庭やオフィスにおける利用の場合よりも高度な機能が要求される。

【０００３】

この種のネットワークアクセスゲートウェイは、ＬＡＮ内の複数のノードを収容することができる。ＬＡＮ内のノードに対しては、自ゲートウェイがＤＨＣＰ(Dynamic Host Configuration Protocol)サーバとなって動的にＩＰアドレスを払い出し、自動的にノードの設定を行うことも可能である。このとき払い出すＩＰアドレスとしては、グローバルＩＰアドレス空間との重複を避けるためにプライベートＩＰアドレスが主に用いられる。

【０００４】

また、この種のネットワークアクセスゲートウェイは、ＷＡＮ側ネットワークインターフェースにＷＡＮ接続用ＩＰアドレス／ネットマスク、デフォルトゲートウェイＩＰアドレスを設定し、さらにＷＡＮアクセスに必要なルーティングテーブルを設定することにより、ＬＡＮ内のノードをＷＡＮに対してアクセスさせることが可能になる。ネットワークアクセスゲートウェイがＬＡＮ内の各ノードからのＤＮＳ(Domain Name System)クエリを中継処理するＤＮＳプロキシ機能を持つ場合は、ＷＡＮにおけるＤＮＳサーバのＩＰアドレスの設定を行うこともある。ＤＨＣＰクライアント機能を有するネットワークアクセスゲートウェイの場合は、上記のＷＡＮ側ネットワークインターフェースにおける設定およびルーティングテーブル、ＤＮＳクエリ転送テーブルにおける各設定パラメータをＷＡＮ内のＤＨＣＰサーバから払い出されることにより、自動的に行うことも可能である。この

他にも、ＷＡＮへのアクセスが、ＷＡＮ内の認証サーバに対してアクセス認証を行うことによって可能になる場合は、ＷＡＮアクセスに必要な設定パラメータが上記認証サーバから払い出される場合もある。ネットワークアクセスゲートウェイと認証サーバとの間で用いられるプロトコルとしては、ＲＡＤＩＵＳプロトコルなどがある。

【０００５】

ＷＡＮアクセスに必要な各設定は、ＬＡＮ内ノードからＷＡＮへのアクセスにおいて、ＬＡＮ内の全てのノードによって共有される。例えば、ネットワークアクセスゲートウェイを介してＷＡＮ側に送信される全てのパケットは、ＷＡＮ接続用ＩＰアドレスにソースＩＰアドレスが変換されて送信される。また、ＷＡＮ側にＬＡＮ内ノードからのアクセスの候補となる仮想的または物理的に分離された網（以下ターゲット網と呼ぶ）が複数存在する場合であっても、ＬＡＮ内の各ノードからアクセスすることが可能なターゲット網は、ネットワークアクセスゲートウェイがアクセス認証されたターゲット網だけである。

【０００６】

上述したネットワークアクセスゲートウェイは、ＬＡＮとＷＡＮとの間で流れるパケットに対してレイヤ３レベル（ＩＰレベル）の処理を行うものであった。さらにレイヤ２レベル（イーサネットレベル：イーサネットは登録商標）の処理を行う装置まで対象を広げると、従来から用いられている認証ＶＬＡＮスイッチも、ネットワークアクセスのためにＬＡＮ内ノードを収容する装置として挙げることができる。認証ＶＬＡＮスイッチは、配下のノードを認証によりアクセスが許可されたＶＬＡＮへ接続するための機能を有するものである。

【特許文献１】特許第３１５３１７３号

【発明の開示】

【発明が解決しようとする課題】

【０００７】

従来技術の第１の問題点は、ネットワークアクセスゲートウェイにおいて、ＬＡＮ内の全てのノードは、ＷＡＮへのアクセスのための環境設定を共有しなければならない点である。

【０００８】

先にも述べたように、ＷＡＮへのアクセスのための環境設定はＬＡＮ内の全てのノードで共有されるため、ネットワークアクセスゲートウェイを介してＷＡＮ側に送信される全てのパケットは、同一のＷＡＮ接続用ＩＰアドレスにソースＩＰアドレスが変換されて送信される。そのため、ＷＡＮ側ではＬＡＮ内の個別のノードをソースＩＰアドレスによって識別することはできないし、ＷＡＮ側からＬＡＮ内の特定のノードを指定して通信を開始することはできない。

【０００９】

また、ＷＡＮ側にアクセスの候補となるターゲット網が複数存在する場合に、ＬＡＮ内のノードごとに異なるターゲット網に対してアクセスさせたい場合であっても、アクセスするターゲット網の設定をＬＡＮ内のノードごとに変えることはできない。

【００１０】

上述した認証ＶＬＡＮスイッチを用いる場合は、ノードごとに認証ベースで異なるＶＬＡＮ（ターゲット網）へアクセスさせることができるが、認証ＶＬＡＮスイッチではレイヤ２レベルのパケット処理しか行えず、ＩＰパケットの転送やＩＰアドレス変換の設定、ＤＮＳメッセージの転送設定など、レイヤ３レベル以上の処理を行うことはできない。例えば、１台のノードが２つ以上のターゲット網に同時にアクセスしようとする場合、レイヤ２レベルの処理ではノードからのパケットをどのターゲット網に転送すればよいか識別することができず、限界がある。すなわち、認証ＶＬＡＮスイッチを用いる方法では、ＬＡＮ内ノードは１つのターゲット網にしかアクセスすることはできない。

【００１１】

従来技術の第２の問題点は、従来技術の第１の問題点が解決され、ＬＡＮ内のノードごとにＷＡＮへのアクセスのための環境設定を変えることができるようになったとしても、

ＬＡＮ内のノードは、ＩＰアドレス領域の重複する複数のターゲット網にアクセスすることができない点である。

【００１２】

例えば、１台のＬＡＮ内のノードが、ターゲット網－Ｘとターゲット網Ｙの２つのターゲット網へのアクセスが許可されたとする。このときもしもターゲット網Ｘとターゲット網Ｙの両方で１０／８というＩＰアドレス領域が用いられる場合、上記ノードから上記ＩＰアドレス領域に含まれる宛先へのＩＰパケットは、ネットワークアクセスゲートウェイにおいてどちらのターゲット網に転送すべきか判断できない。すなわち、従来技術においては、ＩＰアドレス領域の重複する複数のターゲット網にアクセスすることは不可能である。

【００１３】

〔発明の目的〕

本発明の第１の目的は、ＬＡＮ内のノードごとにターゲット網に対する異なるアクセス環境を提供し、これにより、各ノードが任意の数のターゲット網に同時にアクセス可能な環境を提供できるネットワークアクセスゲートウェイを提供することである。

【００１４】

本発明の第２の目的は、ＬＡＮ内のノードがＩＰアドレス領域の重複する複数のターゲット網にアクセスすることを可能とするネットワークアクセスゲートウェイを提供することにある。

【課題を解決するための手段】

【００１５】

本発明にかかる第１のネットワークアクセスゲートウェイは、ＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにするため、

ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイであって、

前記ノードごとに、１つまたは複数の前記ターゲット網へのアクセスのための環境設定を行えることを特徴とする。

【００１６】

本発明にかかる第２のネットワークアクセスゲートウェイは、ターゲット網への不正なアクセスを防ぐため、第１のネットワークアクセスゲートウェイにおいて、

前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする。

【００１７】

本発明にかかる第３のネットワークアクセスゲートウェイは、ＬＡＮ内のノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにすると共に、ターゲット網への不正なアクセスを防ぐため、

ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイであって、

複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証部と、

該端末認証部で認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理部とを備えることを特徴とする。

【００１８】

本発明にかかる第４のネットワークアクセスゲートウェイは、第３のネットワークアクセスゲートウェイにおいて、

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノード

がアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする。

【００１９】

本発明にかかる第５のネットワークアクセスゲートウェイは、第３または第４のネットワークアクセスゲートウェイにおいて、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、

前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第２のエントリが格納される名前解決クエリ転送テーブルとを備え、

前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、

前記ルーティングテーブルに対して第１のエントリを作成し、前記名前解決クエリ転送テーブルに対して第２のエントリを作成することを特徴とする。

【００２０】

本発明にかかる第６のネットワークアクセスゲートウェイは、第５のネットワークアクセスゲートウェイにおいて、

前記名前解決クエリはＤＮＳクエリであり、前記名前解決クエリ転送テーブルはＤＮＳクエリ転送テーブルであることを特徴とする。

【００２１】

本発明にかかる第７のネットワークアクセスゲートウェイは、端末認証部の構成を簡単なものとするため、第３～第６の何れかのネットワークアクセスゲートウェイにおいて、

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする。

【００２２】

本発明にかかる第８のネットワークアクセスゲートウェイは、端末認証部の構成を簡単なものにするため、第３～第６の何れかのネットワークアクセスゲートウェイにおいて、

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証ＶＬＡＮスイッチに問い合わせることにより認証を行うことを特徴とする。

【００２３】

本発明にかかる第９のネットワークアクセスゲートウェイは、セッション管理部の構成を簡単なものにするため、第３～第８の何れかのネットワークアクセスゲートウェイにおいて、

前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得する設定クライアントを有することを特徴とする。

【００２４】

本発明にかかる第１０のネットワークアクセスゲートウェイは、アドレス詐称等によるなりすましを防ぐため、第３～第９の何れかのネットワークアクセスゲートウェイにおいて、

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられることを特徴とする。

【００２５】

本発明にかかる第１１のネットワークアクセスゲートウェイは、ＬＡＮ内のノードがＩＰアドレス領域の重複する複数のターゲット網にアクセスできるようにするため、第３～

第１０のネットワークアクセスゲートウェイの何れかにおいて、
複数の前記ターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求める機能を有するＩＰアドレス領域重複検出部を備えることを特徴とする。

【００２６】
本発明にかかる第１２のネットワークアクセスゲートウェイは、第１１のネットワークアクセスゲートウェイにおいて、
前記セッション管理部は、
前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記ＩＰアドレス領域重複検出部を介して、前記複数のターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求め、
前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第３のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、
重複するＩＰアドレス領域を互いに重複しないＩＰアドレス領域にＩＰアドレス変換するように第１のエントリおよび第３のエントリを設定することを特徴とする。

【００２７】
本発明にかかる第１３のネットワークアクセスゲートウェイは、第１２のネットワークアクセスゲートウェイにおいて、
前記名前解決クエリはＤＮＳクエリであり、前記名前解決応答はＤＮＳ応答であり、前記名前解決クエリ／応答転送テーブルはＤＮＳクエリ／応答転送テーブルであることを特徴とする。

【００２８】
本発明にかかる第１のネットワークアクセスゲートウェイの制御方法は、ネットワークアクセスゲートウェイに収容されているＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにするため、
ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイの制御方法であって、
前記ノードごとに、１つまたは複数の前記ターゲット網へのアクセスのための環境設定を行うことを特徴とする。

【００２９】
本発明にかかる第２のネットワークアクセスゲートウェイの制御方法は、ターゲット網への不正なアクセスを防ぐため、第１のネットワークアクセスゲートウェイの制御方法において、
前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする。

【００３０】
本発明にかかる第３のネットワークアクセスゲートウェイの制御方法は、ＬＡＮ内のノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにすると共に、ターゲット網への不正なアクセスを防止するため、
ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイの制御方法であって、
複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証

ステップと、
該端末認証ステップで認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理ステップとを含むことを特徴とする。
【００３１】
本発明にかかる第４のネットワークアクセスゲートウェイの制御方法は、第３のネットワークアクセスゲートウェイの制御方法において、
前記セッション管理ステップは、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする。
【００３２】
本発明にかかる第５のネットワークアクセスゲートウェイの制御方法は、第３または第４のネットワークアクセスゲートウェイの制御方法において、
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、
前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第２のエントリが格納される名前解決クエリ転送テーブルとを備え、
前記セッション管理ステップでは、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記ルーティングテーブルに対して第１のエントリを作成し、前記名前解決クエリ転送テーブルに対して第２のエントリを作成することを特徴とする。
【００３３】
本発明にかかる第６のネットワークアクセスゲートウェイの制御方法は、第５のネットワークアクセスゲートウェイの制御方法において、
前記名前解決クエリはＤＮＳクエリであり、前記名前解決クエリ転送テーブルはＤＮＳクエリ転送テーブルであることを特徴とする。
【００３４】
本発明にかかる第７のネットワークアクセスゲートウェイの制御方法は、端末認証ステップにおける処理を簡単なものとするため、第３～第６の何れかのネットワークアクセスゲートウェイの制御方法において、
前記端末認証ステップでは、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする。
【００３５】
本発明にかかる第８のネットワークアクセスゲートウェイの制御方法は、端末認証ステップの処理を簡単なものとするため、第３～第６の何れかのネットワークアクセスゲートウェイの制御方法において、
前記端末認証ステップでは、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証ＶＬＡＮスイッチに問い合わせることにより認証を行うことを特徴とする。
【００３６】
本発明にかかる第９のネットワークアクセスゲートウェイの制御方法は、セッション管理部の構成を簡単なものにするため、第３～第８の何れかのネットワークアクセスゲートウェイの制御方法において、
前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのため

の環境設定に必要なパラメータの一部または全てを取得するパラメータ取得ステップを含むことを特徴とする。

【００３７】

本発明にかかる第１０のネットワークアクセスゲートウェイの制御方法は、アドレス詐称等によるなりすましを防ぐため、第３～第９の何れかのネットワークアクセスゲートウェイの制御方法において、

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられることを特徴とする。

【００３８】

本発明にかかる第１１のネットワークアクセスゲートウェイの制御方法は、ＬＡＮ内のノードがＩＰアドレス領域の重複する複数のターゲット網にアクセスできるようにするため、第３～第１０のネットワークアクセスゲートウェイの制御方法の何れかにおいて、

複数の前記ターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求める機能を有するＩＰアドレス領域重複検出ステップを含むことを特徴とする。

【００３９】

本発明にかかる第１２のネットワークアクセスゲートウェイの制御方法は、第１１のネットワークアクセスゲートウェイの制御方法において、

前記セッション管理ステップでは、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記ＩＰアドレス領域重複検出ステップを介して、前記複数のターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第３のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するＩＰアドレス領域を互いに重複しないＩＰアドレス領域にＩＰアドレス変換するように第１のエントリおよび第３のエントリを設定することを特徴とする。

【００４０】

本発明にかかる第１３のネットワークアクセスゲートウェイの制御方法は、第１２のネットワークアクセスゲートウェイの制御方法において、

前記名前解決クエリはＤＮＳクエリであり、前記名前解決応答はＤＮＳ応答であり、前記名前解決クエリ／応答転送テーブルはＤＮＳクエリ／応答転送テーブルであることを特徴とする。

【００４１】

本発明にかかる第１のプログラムは、ネットワークアクセスゲートウェイに収容されるＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにするため、

コンピュータを、ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイとして機能させるためのプログラムであって、

前記コンピュータを、前記ノードごとに、１つまたは複数の前記ターゲット網へのアクセスのための環境設定を行えるネットワークアクセスゲートウェイとして機能させることを特徴とする。

【００４２】

本発明にかかる第２のプログラムは、ターゲット網への不正なアクセスを防ぐため、第１のプログラムにおいて、
前記環境設定は、前記ノードに対して前記ターゲット網へアクセスするための認証が成功したことを契機に行われることを特徴とする。
【００４３】
本発明にかかる第３のプログラムは、ネットワークアクセスゲートウェイに収容されるＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスできるようにすると共に、ターゲット網への不正なアクセスを防止するため、
コンピュータを、ＬＡＮと該ＬＡＮ内のノードからのアクセスの候補となる複数のターゲット網を含むＷＡＮとの境界に設置され、前記ＬＡＮ内のノードを前記ターゲット網に接続させるネットワークアクセスゲートウェイとして機能させるためのプログラムであって、
前記コンピュータを、
複数の前記ターゲット網に対して前記ノードがアクセスするための認証を行う端末認証部、
該端末認証部で認証を行ったアクセスのうち、認証が成功したアクセスのための環境設定を行うセッション管理部として機能させることを特徴とする。
【００４４】
本発明にかかる第４のプログラムは、第３のプログラムにおいて、
前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記認証によってアクセスすることを許可された前記ターゲット網に対して前記ノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成することを特徴とする。
【００４５】
本発明にかかる第５のプログラムは、第３または第４のプログラムにおいて、
前記コンピュータが、
前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、
前記ノードからの名前解決クエリを、前記認証によってアクセスすることを許可された前記ターゲット網に対して転送するための第２のエントリが格納される名前解決クエリ転送テーブルとを備え、
前記セッション管理部は、前記ノードに対する前記ターゲット網へのアクセスのための環境設定として、
前記ルーティングテーブルに対して第１のエントリを作成し、前記名前解決クエリ転送テーブルに対して第２のエントリを作成することを特徴とする。
【００４６】
本発明にかかる第６のプログラムは、第５のプログラムにおいて、
前記名前解決クエリはＤＮＳクエリであり、前記名前解決クエリ転送テーブルはＤＮＳクエリ転送テーブルであることを特徴とする。
【００４７】
本発明にかかる第７のプログラムは、端末認証部における処理を簡単なものとするため、第３～第６の何れかのプログラムにおいて、
前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、
前記ターゲット網内に存在する認証サーバに問い合わせることにより認証を行うことを特徴とする。
【００４８】
本発明にかかる第８のプログラムは、端末認証部の処理を簡単なものとするため、第３～第６の何れかのプログラムにおいて、

前記端末認証部は、前記ノードから前記ターゲット網へアクセスするための認証を前記ターゲット網ごとに行う際に、

前記ターゲット網内に存在し、前記ターゲット網ごとのアクセス認証を行う機能を有する認証ＶＬＡＮスイッチに問い合わせることにより認証を行うことを特徴とする。

【００４９】

本発明にかかる第９のプログラムは、セッション管理部の構成を簡単なものにするため、第３～第８の何れかのプログラムにおいて、

前記コンピュータを、

前記ターゲット網内に存在する、前記ターゲット網にアクセスするために必要な設定パラメータを払い出す機能を有する設定サーバから、前記ターゲット網へのアクセスのための環境設定に必要なパラメータの一部または全てを取得する設定クライアントとして機能させることを特徴とする。

【００５０】

本発明にかかる第１０のプログラムは、アドレス詐称等によるなりすましを防ぐため、第３～第９の何れかのプログラムにおいて、

前記ノードとの接続において、前記ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクが用いられることを特徴とする。

【００５１】

本発明にかかる第１１のプログラムは、ＬＡＮ内のノードがＩＰアドレス領域の重複する複数のターゲット網にアクセスできるようにするため、第３～第１０のプログラムの何れかにおいて、

前記コンピュータを、

複数の前記ターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求めるＩＰアドレス領域重複検出部として機能させることを特徴とする。

【００５２】

本発明にかかる第１２のプログラムは、第１１のプログラムにおいて、

前記セッション管理部は、

前記ノードが前記複数のターゲット網に対してアクセスを行う場合に、前記ＩＰアドレス領域重複検出部を介して、前記複数のターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求め、

前記ノードに対する前記複数のターゲット網へのアクセスのための環境設定として、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間でパケットを送受信するための第１のエントリが格納されるルーティングテーブルと、

前記ノードと、前記認証によってアクセスすることを許可された前記ターゲット網との間で名前解決クエリおよび名前解決応答を送受信するための第３のエントリが格納される名前解決クエリ／応答転送テーブルとに対して、

重複するＩＰアドレス領域を互いに重複しないＩＰアドレス領域にＩＰアドレス変換するように第１のエントリおよび第３のエントリを設定することを特徴とする。

【００５３】

本発明にかかる第１３のプログラムは、第１２のプログラムにおいて、

前記名前解決クエリはＤＮＳクエリであり、前記名前解決応答はＤＮＳ応答であり、前記名前解決クエリ／応答転送テーブルはＤＮＳクエリ／応答転送テーブルであることを特徴とする。

【発明の効果】

【００５４】

本発明にかかる第１のネットワークアクセスゲートウェイによれば、ネットワークアクセスゲートウェイに収容されているＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができる。

【００５５】
その理由は、ネットワークアクセスゲートウェイが、ノード毎に、１つまたは複数のターゲット網へのアクセスのための環境設定を行う構成を備えているからである。
【００５６】
本発明にかかる第２のネットワークアクセスゲートウェイは、ターゲット網への不正なアクセスを防ぐことができるという効果を有する。
【００５７】
その理由は、認証が成功したことを契機として環境設定を行うようにしているからである。
【００５８】
本発明にかかる第３のネットワークアクセスゲートウェイによれば、ネットワークアクセスゲートウェイに収容されているＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができると共に、ターゲット網に対する不正アクセスを防止できるという効果を得ることができる。
【００５９】
その理由は、複数のターゲット網に対してノードがアクセスするための認証を行う端末認証部と、認証が成功したアクセスのための環境設定を行うセッション管理部とを備えているからである。
【００６０】
本発明にかかる第４のネットワークアクセスゲートウェイは、第３のネットワークアクセスゲートウェイと同様の効果を有する。
【００６１】
その理由は、セッション管理部が、端末認証部によってアクセスすることを許可されたターゲット網に対してノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成する構成を有しているからである。
【００６２】
本発明にかかる第５のネットワークアクセスゲートウェイは、第３のネットワークアクセスゲートウェイと同様の効果を有する。
【００６３】
その理由は、セッション管理部が、端末認証部によってアクセスすることが許可されたターゲット網とノードとの間でパケットを送受信するための第１のエントリをルーティングテーブル上に作成すると共に、端末認証部によってアクセスすることを許可されたターゲットに対して名前解決クエリを転送するための第２のエントリを名前解決クリエ転送テーブル上に作成するからである。
【００６４】
本発明にかかる第６のネットワークアクセスゲートウェイは、第３のネットワークアクセスゲートウェイと同様の効果を有する。
【００６５】
その理由は、名前解決クエリがＤＮＳクエリであり、名前解決クエリ転送テーブルがＤＮＳクエリ転送テーブルであるからである。
【００６６】
本発明にかかる第７のネットワークアクセスゲートウェイは、認証機能がターゲット網内の認証サーバに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。
【００６７】
その理由は、ターゲット網内に存在する認証サーバに対して問い合わせを行うことにより、認証を行うようにしているからである。
【００６８】
本発明にかかる第８のネットワークアクセスゲートウェイは、認証機能が認証ＶＬＡＮスイッチに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効

果を有する。

【００６９】

その理由は、認証ＶＬＡＮスイッチに対して問い合わせを行うことにより、認証を行っているからである。

【００７０】

本発明にかかる第９のネットワークアクセスゲートウェイは、環境設定に必要なパラメータが設定サーバに保持されているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。

【００７１】

その理由は、設定サーバから環境設定に必要なパラメータの一部または全てを取得する設定クライアントを備えているからである。

【００７２】

本発明にかかる第１０のネットワークアクセスゲートウェイは、アドレス詐称等によるなりすましを防ぐことができるという効果を有する。

【００７３】

その理由は、ノードとの接続において、ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクを用いるからである。

【００７４】

本発明にかかる第１１のネットワークアクセスゲートウェイは、ネットワークアクセスゲートウェイに収容されているＬＡＮ内のノードが、ＩＰアドレス領域の重複する複数のターゲット網にアクセスできるという効果を有する。

【００７５】

その理由は、複数の前記ターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求めるＩＰアドレス領域重複検出部を備えているからである。

【００７６】

本発明にかかる第１２のネットワークアクセスゲートウェイは、第１１のネットワークアクセスゲートウェイと同様の効果を有する。

【００７７】

その理由は、ＬＡＮ内のノードからの認証要求に基づいて上記ノードが所望するターゲット網へのアクセスが可能になるように設定を行う際に、上記ノードに対してアクセスが許可されたターゲット網間にＩＰアドレス領域の重複がないかどうかを検出し、重複があった場合は、互いに重複しないＩＰアドレス領域にＩＰアドレス変換すべく、ルーティングテーブルエントリ、名前解決クエリ／応答転送テーブルエントリの設定を行うからである。

【００７８】

本発明にかかる第１３のネットワークアクセスゲートウェイは、第１１のネットワークアクセスゲートウェイと同様の効果を有する。

【００７９】

その理由は、名前解決クエリがＤＮＳクエリであり、名前解決応答がＤＮＳ応答であり、名前解決クエリ／応答転送テーブルがＤＮＳクエリ／応答転送テーブルであるからである。

【００８０】

本発明にかかる第１のネットワークアクセスゲートウェイの制御方法によれば、ネットワークアクセスゲートウェイに収容に収容されるＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができる。

【００８１】

その理由は、ネットワークアクセスゲートウェイが、ノード毎に、１つまたは複数のターゲット網へのアクセスのための環境設定を行うからである。

【００８２】
本発明にかかる第２のネットワークアクセスゲートウェイの制御方法は、ターゲット網への不正なアクセスを防ぐことができるという効果を有する。
【００８３】
その理由は、認証が成功したことを契機として環境設定を行うようにしているからである。
【００８４】
本発明にかかる第３のネットワークアクセスゲートウェイの制御方法によれば、ネットワークアクセスゲートウェイに収容されているＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができると共に、ターゲット網に対する不正アクセスを防止できるという効果を得ることができる。
【００８５】
その理由は、複数のターゲット網に対してノードがアクセスするための認証を行う端末認証ステップと、認証が成功したアクセスのための環境設定を行うセッション管理ステップとを含んでいるからである。
【００８６】
本発明にかかる第４のネットワークアクセスゲートウェイの制御方法は、第３のネットワークアクセスゲートウェイの制御方法と同様の効果を有する。
【００８７】
その理由は、セッション管理ステップにおいて、端末認証ステップによってアクセスすることを許可されたターゲット網に対してノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成するようにしているからである。
【００８８】
本発明にかかる第５のネットワークアクセスゲートウェイの制御方法は、第３のネットワークアクセスゲートウェイの制御方法と同様の効果を有する。
【００８９】
その理由は、セッション管理ステップにおいて、アクセスすることが許可されたターゲット網とノードとの間でパケットを送受信するための第１のエントリをルーティングテーブル上に作成する処理と、アクセスすることを許可されたターゲットに対して名前解決クエリを転送するための第２のエントリを名前解決クリエ転送テーブル上に作成する処理を行うからである。
【００９０】
本発明にかかる第６のネットワークアクセスゲートウェイの制御方法は、第３のネットワークアクセスゲートウェイの制御方法と同様の効果を有する。
【００９１】
その理由は、名前解決クエリがＤＮＳクエリであり、名前解決クエリ転送テーブルがＤＮＳクエリ転送テーブルであるからである。
【００９２】
本発明にかかる第７のネットワークアクセスゲートウェイの制御方法は、認証機能がターゲット網内の認証サーバに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。
【００９３】
その理由は、ターゲット網内に存在する認証サーバに対して問い合わせを行うことにより、認証を行うようにしているからである。
【００９４】
本発明にかかる第８のネットワークアクセスゲートウェイの制御方法は、認証機能が認証ＶＬＡＮスイッチに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。
【００９５】
その理由は、認証ＶＬＡＮスイッチに問い合わせることにより認証を行うからである。

【００９６】
本発明にかかる第９のネットワークアクセスゲートウェイの制御方法は、環境設定に必要なパラメータが設定サーバに保持されているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。
【００９７】
その理由は、設定サーバから環境設定に必要なパラメータの一部または全てを取得するパラメータ取得ステップを含んでいるからである。
【００９８】
本発明にかかる第１０のネットワークアクセスゲートウェイの制御方法は、アドレス詐称等によるなりすましを防ぐことができるという効果を有する。
【００９９】
その理由は、ノードとの接続において、ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクを用いるからである。
【０１００】
本発明にかかる第１１のネットワークアクセスゲートウェイの制御方法は、ネットワークアクセスゲートウェイに収容されているＬＡＮ内のノードが、ＩＰアドレス領域の重複する複数のターゲット網にアクセスできるという効果を有する。
【０１０１】
その理由は、複数の前記ターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求めるＩＰアドレス領域重複検出ステップを含んでいるからである。
【０１０２】
本発明にかかる第１２のネットワークアクセスゲートウェイの制御方法は、第１１のネットワークアクセスゲートウェイの制御方法と同様の効果を有する。
【０１０３】
その理由は、ＬＡＮ内のノードからの認証要求に基づいて、上記ノードが所望するターゲット網へのアクセスが可能になるように設定を行う際に、上記ノードに対してアクセスが許可されたターゲット網間にＩＰアドレス領域の重複がないかどうかを検出し、重複があった場合は、互いに重複しないＩＰアドレス領域にＩＰアドレス変換すべく、ルーティングテーブルエントリ、名前解決クエリ／応答転送テーブルエントリの設定を行うからである。
【０１０４】
本発明にかかる第１３のネットワークアクセスゲートウェイの制御方法は、第１１のネットワークアクセスゲートウェイと同様の効果を有する。
【０１０５】
その理由は、名前解決クエリがＤＮＳクエリであり、名前解決応答がＤＮＳ応答であり、名前解決クエリ／応答転送テーブルがＤＮＳクエリ／応答転送テーブルであるからである。
【０１０６】
本発明にかかる第１のプログラムによれば、ネットワークアクセスゲートウェイに収容に収容されるＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができる。
【０１０７】
その理由は、コンピュータを、ノード毎に、１つまたは複数のターゲット網へのアクセスのための環境設定を行うネットワークアクセスゲートウェイとして機能させるからである。
【０１０８】
本発明にかかる第２のプログラムは、ターゲット網への不正なアクセスを防ぐことができるという効果を有する。

【０１０９】
その理由は、認証が成功したことを契機として環境設定を行うようにしているからである。
【０１１０】
本発明にかかる第３のプログラムによれば、ネットワークアクセスゲートウェイに収容されているＬＡＮ内の各ノードが、それぞれ任意の数のターゲット網に同時にアクセスすることが可能になるという効果を得ることができると共に、ターゲット網に対する不正アクセスを防止できるという効果を得ることができる。
【０１１１】
その理由は、コンピュータ上に、複数のターゲット網に対してノードがアクセスするための認証を行う端末認証部と、認証が成功したアクセスのための環境設定を行うセッション管理部とを実現するからである。
【０１１２】
本発明にかかる第４のプログラムは、第３のプログラムと同様の効果を有する。
【０１１３】
その理由は、セッション管理部において、端末認証部によってアクセスすることを許可されたターゲット網に対してノードがアクセスするための仮想インターフェースを、物理インターフェース上に作成するようにしているからである。
【０１１４】
本発明にかかる第５のプログラムは、第３のプログラムと同様の効果を有する。
【０１１５】
その理由は、セッション管理部が、アクセスすることが許可されたターゲット網とノードとの間でパケットを送受信するための第１のエントリをルーティングテーブル上に作成すると共に、アクセスすることを許可されたターゲットに対して名前解決クエリを転送するための第２のエントリを名前解決クリエ転送テーブル上に作成するからである。
【０１１６】
本発明にかかる第６のプログラムは、第３のプログラムと同様の効果を有する。
【０１１７】
その理由は、名前解決クエリがＤＮＳクエリであり、名前解決クエリ転送テーブルがＤＮＳクエリ転送テーブルであるからである。
【０１１８】
本発明にかかる第７のプログラムは、認証機能がターゲット網内の認証サーバに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。
【０１１９】
その理由は、ターゲット網内に存在する認証サーバに対して問い合わせを行うことにより、認証を行うようにしているからである
【０１２０】
本発明にかかる第８のプログラムは、認証機能が認証ＶＬＡＮスイッチに設けられているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。
【０１２１】
その理由は、認証ＶＬＡＮスイッチに問い合わせることにより認証を行うからである。
【０１２２】
本発明にかかる第９のプログラムは、環境設定に必要なパラメータが設定サーバに保持されているようなネットワーク構成の場合にも柔軟に対応できるという効果を有する。
【０１２３】
その理由は、コンピュータ上に、設定サーバから環境設定に必要なパラメータの一部または全てを取得する設定クライアントを実現するようにしているからである。
【０１２４】
本発明にかかる第１０のプログラムは、アドレス詐称等によるなりすましを防ぐことができるという効果を有する。

【０１２５】
その理由は、ノードとの接続において、ノードを一意に識別可能にするために、トンネリングプロトコルによって提供される仮想リンクを用いるからである。
【０１２６】
本発明にかかる第１１のプログラムは、ネットワークアクセスゲートウェイに収容されているＬＡＮ内のノードが、ＩＰアドレス領域の重複する複数のターゲット網にアクセスできるという効果を有する。
【０１２７】
その理由は、コンピュータ上に、複数のターゲット網の各々で利用されているＩＰアドレスの領域が重複するかどうかを調べ、重複があった場合は、重複するＩＰアドレス領域をどのようにＩＰアドレス変換すべきかを求めるＩＰアドレス領域重複検出部を実現するからである。
【０１２８】
本発明にかかる第１２のプログラムは、第１１のプログラムと同様の効果を有する。
【０１２９】
その理由は、ＬＡＮ内のノードからの認証要求に基づいて、上記ノードが所望するターゲット網へのアクセスが可能になるように設定を行う際に、上記ノードに対してアクセスが許可されたターゲット網間にＩＰアドレス領域の重複がないかどうかを検出し、重複があった場合は、互いに重複しないＩＰアドレス領域にＩＰアドレス変換すべく、ルーティングテーブルエントリ、名前解決クエリ／応答転送テーブルエントリの設定を行うからである。
【０１３０】
本発明にかかる第１３のプログラムは、第１１のプログラムと同様の効果を有する。
【０１３１】
その理由は、名前解決クエリがＤＮＳクエリであり、名前解決応答がＤＮＳ応答であり、名前解決クエリ／応答転送テーブルがＤＮＳクエリ／応答転送テーブルであるからである。
【発明を実施するための最良の形態】
【０１３２】
次に本発明の実施の形態について図面を参照して詳細に説明する。
【０１３３】
図１を参照すると、本発明の第１の実施の形態は、端末Ａ１とネットワークアクセスゲートウェイＢ１とスイッチングハブＣ１とターゲットＶＬＡＮ Ｄ１～Ｄ３とによって実現される。ここで、ターゲット網は、以下で詳しく述べるイーサネットのＶＬＡＮによって分離されているものとして説明するが、その他の方法（例えばＩＰｓｅｃ、Ｌ２ＴＰ、ＭＰＬＳ(MultiProtocol Label Switching)等のトンネル技術によるＶＰＮなど）で仮想的または物理的に分離された網であってもよいものとする。
【０１３４】
端末Ａ１は、ターゲットＶＬＡＮ Ｄ１～Ｄ３に含まれる１つ以上のネットワークに対してアクセスを行うＬＡＮ内のノードであり、ＰＣ(Personal Computer)、携帯端末、ワークステーション、ＩＰ電話機などが例に挙げられる。他にも、背景技術で示したような、配下に端末が接続されているネットワークアクセスゲートウェイも、ターゲットＶＬＡＮ Ｄ１～Ｄ３に含まれる１つ以上のネットワークに対してアクセスを行うＬＡＮ内のノードとして挙げることができるが、以下、このようなノードも含めて端末Ａ１として説明する。
【０１３５】
端末Ａ１は、ネットワークアクセスゲートウェイＢ１の配下のＬＡＮに属する端末の１つである。端末Ａ１のＩＰアドレスは、手動で設定されてもよいし、ネットワークアクセスゲートウェイＢ１または他のサーバの提供するＤＨＣＰ(Dynamic Host Configuration Protocol)機能を用いて取得してもよい。端末Ａ１は、ターゲットＶＬＡＮ Ｄ１～Ｄ３に

含まれるネットワークへは通常アクセスすることはできず、アクセスしたい際は、ネットワークアクセスゲートウェイＢ１に対して所望のターゲットＶＬＡＮへのアクセスに対する認証要求を行う。このアクセス認証要求に対応するターゲットＶＬＡＮの数は１つでもよいし、複数であってもよい。認証の結果、アクセスが許可されると、アクセスが許可されたターゲットＶＬＡＮへのアクセスを行うことが可能になる。ネットワークアクセスゲートウェイＢ１に対して認証要求を行う方法の例として、端末Ａ１がネットワークアクセスゲートウェイＢ１の表示するＷｅｂ認証画面に、アクセスしたいターゲットＶＬＡＮにおけるユーザＩＤおよびパスワードを入力する方法などが挙げられる。

【０１３６】

ネットワークアクセスゲートウェイＢ１は、端末Ａ１をはじめとするＬＡＮ内の端末とＷＡＮ側のネットワークであるターゲットＶＬＡＮ Ｄ１～Ｄ３とを接続する機能を有するアクセスゲートウェイであり、認証ベースでＬＡＮ内の端末ごとに異なるネットワークアクセス環境を提供する機能を有する。ネットワークアクセスゲートウェイＢ１は、その内部構成として、端末認証部Ｂ１１とセッション管理部Ｂ１２とルーティングテーブルＢ１３とルーティング処理部Ｂ１４とＤＮＳクエリ転送テーブルＢ１５とＤＮＳプロキシ部Ｂ１６とインターフェースドライバＢ１７とネットワークインターフェースＢ１８とを含む。

【０１３７】

スイッチングハブＣ１は、ネットワークアクセスゲートウェイＢ１に対して複数のターゲットＶＬＡＮが収容できるようにするためにネットワークアクセスゲートウェイＢ１とターゲットＶＬＡＮ Ｄ１～Ｄ３との間に設置される。このようにネットワークアクセスゲートウェイＢ１から同一リンク上に複数のネットワークセグメントを収容できるようにするために、イーサネットにおけるＶＬＡＮ機能（ＩＥＥＥ８０２．１ｑで定義されている）が利用される。ＶＬＡＮ機能を使った場合、ネットワークアクセスゲートウェイＢ１とターゲットＶＬＡＮ Ｄ１～Ｄ３との間の通信は、スイッチングハブＣ１やネットワークアクセスゲートウェイＢ１においてＶＬＡＮタグの値を見ることにより、どのターゲットＶＬＡＮに対応するパケットであるかを識別可能となる。

【０１３８】

ターゲットＶＬＡＮ Ｄ１～Ｄ３は、端末Ａ１がアクセスを行うターゲットとなるネットワーク（ターゲット網）である。図１に示した例では、３つのターゲットＶＬＡＮが記載されているが、任意の数のターゲットＶＬＡＮが存在してよい。端末Ａ１はネットワークアクセスゲートウェイＢ１に認証要求を出し、所望のターゲットＶＬＡＮに対するアクセス認証を行う。アクセスが許可されると、ターゲットＶＬＡＮ内およびこのターゲットＶＬＡＮを経由してアクセス可能な網内のＷｅｂサーバ、メールサーバ等の各種サーバ、またはその他の端末と通信することにより、通信サービスを受けることができる。以下、簡単のために、ターゲットＶＬＡＮを経由してアクセス可能な網も含めてターゲットＶＬＡＮとよぶ。

【０１３９】

次にネットワークアクセスゲートウェイＢ１の構成について以下に詳細に記す。

【０１４０】

端末認証部Ｂ１１は、端末Ａ１がネットワークアクセスゲートウェイＢ１に対して行う認証要求を処理し、その結果、端末Ａ１から所望のターゲットＶＬＡＮへのアクセスが可能であると判断した場合、セッション管理部Ｂ１２に対して端末Ａ１から所望のターゲットＶＬＡＮへのアクセスを行うために必要な設定を行うよう指示し、さらに端末Ａ１に対して、アクセスが許可された旨を通知する。また、認証の結果、アクセスが不可能であると判断した場合は、端末Ａ１に対してアクセスが許可されなかった旨を通知する。

【０１４１】

セッション管理部Ｂ１２に対して端末Ａ１から所望のターゲットＶＬＡＮへのアクセスを行うために必要な設定を行うよう指示する場合、設定に必要なパラメータを端末認証部Ｂ１１からセッション管理部Ｂ１２に対して渡す。このために必要なパラメータは、端末

認証部Ｂ１１に予め登録されていてもよいし、あるいはこのパラメータを保持する外部のサーバから取得してもよい。設定に必要なパラメータを外部サーバから取得する場合は、端末認証部Ｂ１１はパラメータを取得する機能を有する。

【０１４２】

セッション管理部Ｂ１２は、端末Ａ１をはじめとするＬＡＮ内端末からのターゲットＶＬＡＮへのアクセスが認証により許可されると、端末ごとに異なるネットワークアクセス環境が提供できるようにルーティングテーブルＢ１３、ＤＮＳクエリ転送テーブルＢ１５、インターフェースドライバＢ１７に対して必要な設定を行う機能を有する。以下に具体的な設定内容を記す。

【０１４３】

本実施の形態においては、端末ごとに異なるネットワークアクセス環境が提供できるように、ターゲットＶＬＡＮへのアクセスが許可された端末ごとに、アクセスが許可されたターゲットＶＬＡＮ数分だけのインターフェースが割り当てられる。そこで、認証により端末からターゲットＶＬＡＮへのアクセスが許可されると、セッション管理部Ｂ１２は、インターフェースドライバＢ１７へ指示を出し、アクセスが許可されたターゲットＶＬＡＮに対応する仮想インターフェースを作成する。具体的には、作成する仮想インターフェースの識別子（ｅｔｈ０：１など）、ＭＡＣアドレス、接続用ＩＰアドレス／ネットマスクを設定する。ＶＬＡＮタグの使用によってターゲットＶＬＡＮが仮想的に区切られている場合は、アクセスするターゲットＶＬＡＮに対応するＶＬＡＮタグＩＤも同時に設定する。

【０１４４】

次にルーティングテーブルＢ１３に対し、アクセスが許可されたターゲットＶＬＡＮへのルーティングテーブルエントリを設定する。具体的には、ターゲットＶＬＡＮごとに、端末からの入力インターフェース、端末のＩＰアドレス（ソースＩＰアドレス）、ターゲットＶＬＡＮへアクセスするときの接続用ＩＰアドレス（宛先ＩＰアドレス）、ターゲットＶＬＡＮのＩＰアドレス領域（ソースＩＰアドレス）、ターゲットＶＬＡＮにおけるゲートウェイＩＰアドレス及びターゲットＶＬＡＮへの出力インターフェースを設定する。更に、ターゲットＶＬＡＮ毎に、ターゲットＶＬＡＮからの入力インターフェース、ターゲットＶＬＡＮのＩＰアドレス領域（ソースＩＰアドレス）、端末へアクセスするときの接続用ＩＰアドレス（宛先ＩＰアドレス）、端末のＩＰアドレス（宛先ＩＰアドレス）、端末への出力インターフェースを設定する。

【０１４５】

さらに、ＤＮＳクエリ転送テーブルＢ１５に対し、端末からのＤＮＳクエリをターゲットＶＬＡＮへ転送するためのエントリを設定する。具体的には、端末からの入力インターフェース、端末のＩＰアドレス、ターゲットＶＬＡＮに対応するドメインネーム領域およびＩＰアドレス領域、ターゲットＶＬＡＮにおけるＤＮＳサーバのＩＰアドレス、ターゲットＶＬＡＮへの出力インターフェースを設定する。

【０１４６】

ルーティングテーブルＢ１３は、ルーティング処理部Ｂ１４が行うパケットの転送処理のルールが記述されているテーブルである。ルーティングテーブルＢ１３の設定は、セッション管理部Ｂ１２によってなされることが可能である。図２にルーティングテーブルＢ１３の例を示す。図２を参照すると、入力されたパケットに対して、このパケットを出力するための方法が登録されている。例えば、インターフェースｅｔｈ１から入力し、ソースＩＰアドレスが１９２．１６８．０．２であるパケットに対しては、宛先ＩＰアドレスに応じて出力方法が異なり、宛先ＩＰアドレスが先頭ビットに８ビットのマスクをかけると１０．０．０．０になる場合（１０／８は先頭８ビットにマスクをかけると１０．０．０．０となるＩＰアドレス群のことを示す。すなわち１０．１．２．３や１０．２．３．４などが当てはまる。）、ソースＩＰアドレスを１０．１．１．１に書き換え、インターフェースｅｔｈ０：０から出力する。この場合のゲートウェイのＩＰアドレスは１０．１．１．２５４である。また、宛先ＩＰアドレスが先頭ビットに８ビットのマスクをかける

と２０．０．０．０になる場合は、ソースＩＰアドレスを２０．１．１．１に書き換え、インターフェースｅｔｈ０：１から出力する。この場合のゲートウェイのＩＰアドレスは２０．１．１．２５４である。別のエントリでは、インターフェースｅｔｈ０：０から入力した、１０／８のＩＰアドレス領域に含まれるソースＩＰアドレス、１０．１．１．１の宛先ＩＰアドレスをもつパケットは、宛先ＩＰアドレスを１９２．１６８．０．２に書き換え、インターフェースｅｔｈ１から出力することが示されている。なお、図２において、ｅｔｈ１は、端末Ａ１側の物理インターフェースを表し、ｅｔｈ０：０～ｅｔｈ０：４は、ターゲットＶＬＡＮ側の物理インターフェースｅｔｈ０上に作成された仮想インターフェースを表している。

【０１４７】

ここで、ルーティングテーブルＢ１３における入力パケットの識別方法として、インターフェース識別子、ソースＩＰアドレス、宛先ＩＰアドレスの他に、ソースＭＡＣアドレスなどのパケットに含まれる他のフィールドの情報を用いてもよい。また、ＩＰｓｅｃやＬ２ＴＰやＭＰＬＳなどの仮想リンクをエミュレートするトンネリングプロトコルを用いている場合は、仮想リンクに対応する仮想インターフェースの識別子を用いることも可能である。

【０１４８】

ルーティング処理部Ｂ１４は、ネットワークアクセスゲートウェイＢ１が受信したパケットを、ルーティングテーブルＢ１３に登録されているパケット転送ルールにしたがって転送を行う機能を有する。

【０１４９】

ＤＮＳクエリ転送テーブルＢ１５は、端末Ａ１が送信したＤＮＳクエリをＤＮＳプロキシ部Ｂ１６がどのように転送するかを示すルールが登録されており、セッション管理部Ｂ１２によって設定されることが可能である。ＤＮＳクエリ転送テーブルＢ１５の例を図３に示す。図３を参照すると、インターフェースｅｔｈ１から入力し、ソースＩＰアドレスが１９２．１６８．０．２であるＤＮＳクエリに対しては、クエリ内容に応じてＤＮＳクエリの転送方法が異なり、ａａａ．ｃｏｍドメインに含まれるドメインネーム（ｗｗｗ．ａａａ．ｃｏｍやｆｔｐ．ｘｘｘ．ａａａ．ｃｏｍなど）に対応するＩＰアドレスを解決するＤＮＳクエリおよび１０／８のＩＰアドレスプレフィクスに含まれるＩＰアドレスに対応するドメインネームを解決するＤＮＳクエリの場合は、ソースＩＰアドレスを１０．１．１．１とし、出力インターフェースｅｔｈ０：０から、１０．１．２．３に対応するＤＮＳサーバへＤＮＳクエリを転送し、ｂｂｂ．ｃｏｍドメインに含まれるドメインネームに対応するＩＰアドレスを解決するＤＮＳクエリおよび２０／８のＩＰアドレスプレフィクスに含まれるＩＰアドレスに対応するドメインネームを解決するＤＮＳクエリの場合は、ソースＩＰアドレスを２０．１．１．１とし、出力インターフェースｅｔｈ０：１から、２０．１．２．３に対応するＤＮＳサーバへＤＮＳクエリを転送するというルールが示されている。

【０１５０】

ここで、ＤＮＳクエリ転送テーブルＢ１５における入力ＤＮＳクエリの識別方法として、インターフェース識別子、ソースＩＰアドレス、入力クエリ内容の他に、ソースＭＡＣアドレスなどのパケットに含まれる他のフィールドの情報を用いてもよい。また、ＩＰｓｅｃやＬ２ＴＰやＭＰＬＳなどの仮想リンクをエミュレートするトンネリングプロトコルを用いている場合は、仮想リンクに対応する仮想インターフェースの識別子を用いることも可能である。

【０１５１】

ＤＮＳプロキシ部Ｂ１６は、端末Ａ１が送信したＤＮＳクエリを一旦受信し、ＤＮＳクエリ転送テーブルＢ１５に登録されているルールにしたがって、上記ＤＮＳクエリを送信した端末Ａ１を識別してさらに送信した端末Ａ１およびクエリ内容（すなわちクエリに含まれるドメインネームまたはＩＰアドレス）に基づいてターゲットＶＬＡＮ内のＤＮＳサーバに対して上記ＤＮＳクエリを転送する。さらにターゲットＶＬＡＮ内のＤＮＳサーバ

から受信したＤＮＳ応答を、ＤＮＳクエリを送信した端末Ａ１に対して転送する。

【０１５２】

インターフェースドライバＢ１７は、ネットワークアクセスゲートウェイＢ１のもつネットワークインターフェースＢ１８を制御するドライバモジュールであり、データリンクレイヤレベルのパケット送受信処理を行う。インターフェースドライバＢ１７は、ネットワークインターフェースＢ１８内に複数の仮想的なインターフェースを作成する機能を有し、この機能により、物理的なネットワークインターフェース上に任意の数の仮想インターフェースを持たせることができる。また、各仮想インターフェースごとにＭＡＣアドレス、ＶＬＡＮタグＩＤ、ＩＰアドレス、ネットマスクの設定を行うことができる。図４に物理的なネットワークインターフェース上に複数の仮想インターフェースが設定される例をインターフェース設定テーブル１０３として示す。図４を参照すると、ｅｔｈ０で示される物理インターフェース上に、ｅｔｈ０：０，ｅｔｈ０：１，ｅｔｈ０：２，ｅｔｈ０：３，ｅｔｈ０：４で示される５つの仮想インターフェースが設定されており、それぞれに異なるＭＡＣアドレス、ＶＬＡＮタグＩＤ、ＩＰアドレス、ネットマスクが設定されている。仮想インターフェースの設定は、セッション管理部Ｂ１２によってなされることが可能である。

【０１５３】

ここで、インターフェースドライバＢ１７でもつことの可能な仮想インターフェースは、ＭＡＣアドレスまたはＶＬＡＮタグＩＤで区別できる仮想インターフェースだけではなく、ＩＰｓｅｃやＬ２ＴＰやＭＰＬＳなどの仮想リンクをエミュレートするトンネリングプロトコルの仮想リンクのインターフェースであってもよい。例えば、図４の例では、ＬＡＮ側のインターフェースはｅｔｈ１の１つしかないが、ＬＡＮ内の各端末に対して個別にＩＰｓｅｃトンネルが作成される場合は、各端末に対応する仮想リンクのインターフェースがＬＡＮ側の仮想インターフェースとして設定される。あるいは、ターゲット網がＭＰＬＳのラベルによって仮想的に分離されている場合は、ＷＡＮ側の仮想インターフェースとしてＭＰＬＳのインターフェースが用いられる。このようなトンネリングプロトコルを用いる効果としては、アドレス詐称等によるなりすましを防ぎ、ネットワークアクセスゲートウェイＢ１において、接続されている端末Ａ１を確実かつ一意に識別できるようになることが挙げられる。

【０１５４】

次に、図５を参照して、本実施の形態において、端末Ａ１がネットワークアクセスゲートウェイＢ１に対して、ＷＡＮ内のターゲットＶＬＡＮへアクセスするための認証要求を出した場合のネットワークアクセスゲートウェイＢ１における動作について詳細に説明する。

【０１５５】

ここでは、端末Ａ１はターゲットＶＬＡＮ Ｄ１とターゲットＶＬＡＮ Ｄ２の２つのターゲットＶＬＡＮに対してアクセスするための認証要求を出すものとする。ターゲットＶＬＡＮ Ｄ１およびＤ２の識別子は、それぞれａａａ．ｃｏｍ、ｂｂｂ．ｃｏｍであり、ドメインネーム領域、ＩＰアドレス領域はそれぞれａａａ．ｃｏｍ、１０／８およびｂｂｂ．ｃｏｍ、２０／８であるとする。また、ターゲットＶＬＡＮ Ｄ１とターゲットＶＬＡＮ Ｄ２はそれぞれＶＬＡＮタグＩＤが１００、２００のＶＬＡＮでスイッチングハブＣ１によって論理的に分割されているものとする。端末Ａ１は、ネットワークアクセスゲートウェイＢ１のインターフェースｅｔｈ１の配下に存在し、１９２．１６８．０．２のＩＰアドレスをもつものとする。

【０１５６】

端末Ａ１がＷＡＮ内のターゲットＶＬＡＮへアクセスするための認証要求をネットワークアクセスゲートウェイＢ１へ送信すると、端末認証部Ｂ１１がこの認証要求を受信する。この認証要求には、端末Ａ１がアクセスしようとしているターゲットＶＬＡＮを示す識別子と、認証のために必要なパラメータ（ＩＤ、パスワードなど）が含まれており、認証要求に含まれるパラメータに基づいてユーザがアクセス可能であるかどうかの認証を行う

（図５のステップＳ１０１）。例えば認証要求に、［ｔａｒｏ＠ａａａ．ｃｏｍ／ｐａｓｓ－１］［ｔａｒｏ＠ｂｂｂ．ｃｏｍ／ｐａｓｓ－２］というメッセージが埋め込まれている場合は、ａａａ．ｃｏｍに対応するドメイン（ターゲットＶＬＡＮ Ｄ１）に対してｔａｒｏ／ｐａｓｓ－１というユーザＩＤ／パスワードで、ｂｂｂ．ｃｏｍに対応するドメイン（ターゲットＶＬＡＮ Ｄ２）に対してｔａｒｏ／ｐａｓｓ－２というユーザＩＤ／パスワードでアクセス認証を行いたいということを示すものである。ここでは、各ターゲットＶＬＡＮごとにユーザＩＤ／パスワードが必要となる例について示したが、他にも、１つのユーザＩＤ／パスワードで複数のターゲットＶＬＡＮに対するアクセス認証を行う方法も可能である。

【０１５７】

ステップＳ１０１におけるアクセス認証の結果、端末Ａ１から所望するターゲットＶＬＡＮへのアクセスを許可できると判断された場合（ステップＳ１０２がイエス）、端末認証部Ｂ１１は、セッション管理部Ｂ１２に対して、アクセスが許可されたターゲットＶＬＡＮへのアクセスに必要な設定を行うよう指示する（ステップＳ１０３）。このとき、端末Ａ１に対応する入力インターフェース（ｅｔｈ１）、ＩＰアドレス（１９２．１６８．０．２）とともに、アクセスが許可されたターゲットＶＬＡＮの識別子（ａａａ．ｃｏｍとｂｂｂ．ｃｏｍ）、およびそれぞれのターゲットＶＬＡＮに対するＶＬＡＮタグＩＤ（１００と２００）、接続用ＩＰアドレス／ネットマスク（１０．１．１．１／２５５．２５５．２５５．０と２０．１．１．１／２５５．２５５．２５５．０）、ゲートウェイＩＰアドレス（１０．１．１．２５４と２０．１．１．２５４）、ドメインネーム領域（ａａａ．ｃｏｍとｂｂｂ．ｃｏｍ）、ＩＰアドレス領域（１０／８と２０／８）、ＤＮＳサーバＩＰアドレス（１０．１．２．３と２０．１．２．３）が設定に必要なパラメータとして渡される。上記カッコ内に記載されたパラメータは、本実施の形態において渡される実際のパラメータの例である。以下、上記カッコ内に記載されたパラメータが渡されたものとして説明を行う。

【０１５８】

ステップＳ１０３の結果、セッション管理部Ｂ１２はまず、アクセスが許可されたターゲットＶＬＡＮに対応する仮想インターフェースを作成するようにインターフェースドライバＢ１７対して指示を出す（ステップＳ１０４）。ここでは、ターゲットＶＬＡＮ Ｄ１へのアクセスのために図４におけるｅｔｈ０：０のエントリで示される仮想インターフェースが作成され、ターゲットＶＬＡＮ Ｄ２へのアクセスのためにｅｔｈ０：１のエントリで示される仮想インターフェースが作成される。

【０１５９】

ステップＳ１０４の次に、セッション管理部Ｂ１２は、アクセスが許可されたターゲットＶＬＡＮへ端末Ａ１からのパケットを転送するためのルーティングテーブルエントリをルーティングテーブルＢ１３に対して作成する（ステップＳ１０５）。ここでは、図２の入力ソースＩＰアドレスが１９２．１６８．０．２に対応するエントリが作成される。このエントリには、アクセスが許可された各ターゲットＶＬＡＮに対応して、ターゲットＶＬＡＮ Ｄ１宛のパケット（宛先ＩＰアドレスが１０／８の場合）のルーティング方法と、ターゲットＶＬＡＮ Ｄ２宛のパケット（宛先ＩＰアドレスが２０／８の場合）のルーティング方法がそれぞれ登録されている。更に、ここでは、図２のインターフェースｅｔｈ０：０及びインターフェースｅｔｈ０：１に対応するエントリも作成される。インターフェースｅｔｈ０：０に対応するエントリには、ターゲットＶＬＡＮ Ｄ１から端末Ａ１へのパケットのルーティング方法が登録され、インターフェースｅｔｈ０：１に対応するエントリには、ターゲットＶＬＡＮ Ｄ２から端末Ａ１へのパケットのルーティング方法が登録されている。

【０１６０】

ステップＳ１０５の次に、セッション管理部Ｂ１２は、端末Ａ１が送信したＤＮＳクエリを転送するためのエントリをＤＮＳクエリ転送テーブルＢ１５に対して設定する（ステップＳ１０６）。ここでは、図３の入力ソースＩＰアドレスが１９２．１６８．０．２に

対応するエントリが作成される。アクセスが許可された各ターゲットＶＬＡＮに対応して、ターゲットＶＬＡＮ　Ｄ１へのＤＮＳクエリ（ドメインネーム領域がａａａ．ｃｏｍ、ＩＰアドレス領域が１０／８である場合）の転送方法と、ターゲットＶＬＡＮ　Ｄ２へのＤＮＳクエリ（ドメインネーム領域がａａａ．ｃｏｍ、ＩＰアドレス領域が１０／８である場合）の転送方法がそれぞれ登録されている。

【０１６１】

ステップＳ１０６の後、セッション管理部Ｂ１２は、端末認証部Ｂ１１に対して指示された設定が終了したことを通知し、端末認証部Ｂ１１は、アクセス認証成功を伝えるメッセージを端末Ａ１に対して応答する（ステップＳ１０７）。このメッセージが応答されると、端末Ａ１は認証により許可されたターゲットＶＬＡＮへのアクセスを行うことが可能となる。

【０１６２】

また、ステップＳ１０１におけるアクセス認証の結果、端末Ａ１から所望するターゲットＶＬＡＮへのアクセスを許可できないと判断された場合、端末認証部Ｂ１１は、アクセス認証失敗を伝えるメッセージを端末Ａ１に対して応答する（ステップＳ１０８）。

【０１６３】

以上、本実施の形態におけるネットワークアクセスゲートウェイＢ１における動作について説明した。

【０１６４】

以下、本実施の形態から考えられる他の実施の形態についても併せて説明する。

【０１６５】

１つ目は、端末認証部Ｂ１１が端末Ａ１からの認証要求に対して直接認証を行うのではなく、各ターゲットＶＬＡＮ　Ｄ１～Ｄ３に存在する認証サーバＥ１～Ｅ３に対して認証要求を転送し、認証サーバＥ１～Ｅ３が実際の認証を行う形態である（図６を参照）。

【０１６６】

この場合、端末認証部Ｂ１１は、端末Ａ１から受信した認証要求を解析し、端末Ａ１がアクセスしたいターゲットＶＬＡＮに対応する認証サーバへ上記認証要求を転送する。例えば端末認証部Ｂ１１が端末Ａ１から受信した認証要求に、［ｔａｒｏ＠ａａａ．ｃｏｍ／ｐａｓｓ－１］［ｔａｒｏ＠ｂｂｂ．ｃｏｍ／ｐａｓｓ－２］というメッセージが埋め込まれている場合は、ａａａ．ｃｏｍに対応するターゲットＶＬＡＮ内の認証サーバへは、［ｔａｒｏ／ｐａｓｓ－１］の部分を転送し、ｂｂｂ．ｃｏｍに対応するターゲットＶＬＡＮ内の認証サーバへは、［ｔａｒｏ／ｐａｓｓ－２］の部分を転送するという動作を端末認証部Ｂ１１が行う。セッション管理部Ｂ１２が行う設定に必要なパラメータは、端末認証部Ｂ１１が認証サーバＥ１～Ｅ３から取得する。

【０１６７】

２つ目は、ネットワークアクセスゲートウェイＢ１が認証ＶＬＡＮスイッチＣ２によってターゲットＶＬＡＮ　Ｄ１～Ｄ３と接続されており、端末認証部Ｂ１１が端末Ａ１からの認証要求に対して直接認証を行うのではなく、認証ＶＬＡＮスイッチＣ２に対して認証要求を転送し、認証ＶＬＡＮスイッチＣ２（もしくは認証ＶＬＡＮスイッチに接続されている外部の認証サーバ；この外部の認証サーバは多段構成になっていてもよい）が実際の認証を行う形態である（図７を参照）。このような認証ＶＬＡＮスイッチＣ２の例として、ＩＥＥＥ８０２．１ｘに対応した認証ＶＬＡＮスイッチが挙げられる。

【０１６８】

この場合、端末認証部Ｂ１１は、端末Ａ１から受信した認証要求を認証ＶＬＡＮスイッチＣ２に対して送信する。ＩＥＥＥ８０２．１ｘに対応した認証ＶＬＡＮスイッチが用いられる場合は、認証メッセージを送受信するプロトコルとして、ＥＡＰＯＬ(Extensible Authentication Protocol Over Lans)が用いられるため、端末Ａ１と端末認証部Ｂ１１との間で送受信するためのプロトコルはＥＡＰＯＬ形式に変換される。端末Ａ１が２つ以上のターゲットＶＬＡＮへの認証要求を送信している場合は、端末認証部Ｂ１１は認証を要求されている各ターゲットＶＬＡＮ　Ｄ１～Ｄ３ごとに対応するＥＡＰＯＬフレームを認

証ＶＬＡＮスイッチＣ２に対して送信する。

【０１６９】

３つ目は、端末Ａ１から所望のターゲットＶＬＡＮへのアクセスを行うために必要な全ての設定パラメータを端末認証部Ｂ１１からセッション管理部Ｂ１２へ渡すのではなく、一部のパラメータを、ターゲットＶＬＡＮ内の設定サーバから、ネットワークアクセスゲートウェイが備える設定クライアントが自動的に取得して設定を行う形態である。この種の設定サーバ、設定クライアントとしては、それぞれＤＨＣＰサーバ、ＤＨＣＰクライアントが一般的に用いられる。他にも、ＩＰｖ６で用いられるＮＤＰ(Neighbor Discovery Protocol)機能を用いる方法もある。以下、ＤＨＣＰサーバ、ＤＨＣＰクライアントが用いられる場合を例に挙げて説明する。

【０１７０】

この場合、図８に示すように、各ターゲットＶＬＡＮ Ｄ１～Ｄ３内にはＤＨＣＰサーバ（ＤＨＣＰサーバＦ１～Ｆ３）が存在し、さらにネットワークアクセスゲートウェイＢ１の代わりに、ＤＨＣＰクライアントＢ１９を有するネットワークアクセスゲートウェイＢ２が用いられる。ＤＨＣＰクライアントＢ１９は、ＤＨＣＰサーバＦ１～Ｆ３からターゲットＶＬＡＮ Ｄ１～Ｄ３へのアクセスに必要なパラメータを取得し、取得したパラメータをセッション管理部Ｂ１２に渡す。セッション管理部Ｂ１２は、渡された設定パラメータを用いて、インターフェースドライバＢ１７、ルーティングテーブルＢ１３、ＤＮＳクエリ転送テーブルＢ１５に対して設定を行う。

【０１７１】

さらにこの場合のネットワークアクセスゲートウェイＢ２の動作を図９に示す。ステップ１０４において、ターゲットＶＬＡＮごとに仮想インターフェースを作成した後、アクセスが許可された各ターゲットＶＬＡＮ内のＤＨＣＰサーバから設定パラメータを取得して（ステップＳ１０９）から、セッション管理部Ｂ１２が上記仮想インターフェースにおけるＩＰアドレス／ネットマスクの設定（ステップＳ１１０）、ルーティングテーブルエントリの作成（ステップＳ１０５）、ＤＮＳクエリ転送テーブルの作成（ステップＳ１０６）を行う点が、先に図５で示したネットワークアクセスゲートウェイＢ１の動作と異なる。ここで、ステップＳ１０４の時点では、作成された仮想インターフェースに対してＩＰアドレス／ネットマスクは設定されていないことに注意する。

【０１７２】

ＤＨＣＰサーバから取得できるパラメータは、接続用ＩＰアドレス／ネットマスク、デフォルトゲートウェイＩＰアドレス、ＩＰアドレス領域が主なものである。その他、ＭＡＣアドレスなど、設定に必要なパラメータでＤＨＣＰサーバから取得することができないものに関しては、端末認証部Ｂ１１から渡される。

【０１７３】

４つ目は、ネットワークアクセスゲートウェイＢ１において、ＤＮＳプロトコルにおけるクエリ／応答だけではなく、その他の種類の名前解決プロトコルにおけるクエリ／応答のプロキシ処理が行われる形態である。その他の種類の名前解決プロトコルとして、ＬＤＡＰ(Lightweight Directory Access Protocol)やＷＩＮＳ(Windows Internet Name Service：Windowsは登録商標)プロトコルなどが挙げられる。この場合は、本実施の形態におけるＤＮＳクエリ転送テーブルＢ１５およびＤＮＳプロキシ部Ｂ１６の代わりあるいは追加として、名前解決クエリ転送テーブルおよび名前解決プロキシ部が用いられ、名前解決クエリ転送テーブルおよび名前解決プロキシ部がその他の種類の名前解決プロトコルに対するプロキシ処理を行う。

【０１７４】

なお、図１、図６、図７に示したネットワークアクセスゲートウェイＢ１や、図８に示したネットワークアクセスゲートウェイＢ２はコンピュータによって実現可能である。ネットワークアクセスゲートウェイＢ１をコンピュータによって実現する場合には、コンピュータをネットワークアクセスゲートウェイＢ１として機能させるためのプログラムを記録した記録媒体（ディスク、半導体メモリ、その他の記録媒体）を用意しておく。コンピ

ュータは、この記録媒体に記録されたプログラムを読み込み、自身の動作を制御することにより、自コンピュータ上に、端末認証部Ｂ１１、セッション管理部Ｂ１２、ルーティングテーブルＢ１３、ルーティング処理部Ｂ１４、ＤＮＳクエリ転送テーブルＢ１５、ＤＮＳプロシキ部Ｂ１６、インターフェースドライバＢ１７、ネットワークインターフェースＢ１８を実現する。また、ネットワークアクセスゲートウェイＢ２をコンピュータによって実現する場合には、コンピュータをネットワークアクセスゲートウェイＢ２として機能させるためのプログラムを記録した記録媒体（ディスク、半導体メモリ、その他の記録媒体）を用意しておく。コンピュータは、この記録媒体に記録されたプログラムを読み込み、自身の動作を制御することにより、自コンピュータ上に、端末認証部Ｂ１１、セッション管理部Ｂ１２、ルーティングテーブルＢ１３、ルーティング処理部Ｂ１４、ＤＮＳクエリ転送テーブルＢ１５、ＤＮＳプロシキ部Ｂ１６、インターフェースドライバＢ１７、ネットワークインターフェースＢ１８、ＤＨＣＰクライアントＢ１９を実現する。

【０１７５】

次に本実施の形態の効果について説明する。

【０１７６】

本実施の形態では、ネットワークアクセスゲートウェイＢ１は、ＬＡＮ内の端末Ａ１からの認証要求に基づき、端末Ａ１が所望するターゲットＶＬＡＮへのアクセスが可能になるように、インターフェースドライバＢ１７に対して仮想インターフェースを作成するとともに、端末Ａ１が送受信するパケットを転送するための設定をルーティングテーブルＢ１３に対して行い、さらに端末Ａ１が送信するＤＮＳクエリを転送するための設定をＤＮＳクエリ転送テーブルＢ１５に対して行う。

【０１７７】

従来技術では、ネットワークアクセスゲートウェイにおけるＷＡＮ側のインターフェースは、ＬＡＮ内の全ての端末に対して共有される。すわなち、ＬＡＮ内の全ての端末に対して同一のＷＡＮ側の設定が用いられねばならなかった。本実施の形態により、ＬＡＮ内端末からの認証に基づいて、この端末のＷＡＮアクセスのために個別の仮想インターフェース、ルーティングテーブルエントリ、ＤＮＳクエリ転送テーブルエントリが作成されるため、ＬＡＮ内の端末ごとに異なるターゲット網に対するアクセス環境を提供することが可能になる。また、仮想インターフェース、ルーティングテーブルエントリ、ＤＮＳクエリ転送テーブルエントリの設定は、端末に対してアクセスが許可された任意の数のターゲット網に対して行われるため、端末に対して任意の数のターゲット網に同時にアクセス可能な環境を提供することが可能となる。

【０１７８】

次に、本発明の第２の実施の形態について図面を参照して詳細に説明する。

【０１７９】

図１０を参照すると、本発明の第２の実施の形態は、ネットワークアクセスゲートウェイＢ１の代わりに、ネットワークアクセスゲートウェイＢ３が用いられる点が図１に示した本発明の第１の実施の形態における構成と異なる。ネットワークアクセスゲートウェイＢ３は、ＤＮＳクエリ転送テーブルＢ１５の代わりにＤＮＳクエリ／応答転送テーブルＢ２１を有する点、ルーティングテーブルＢ１３の代わりにルーティングテーブルＢ１３ａを有する点、およびＩＰアドレス領域重複検出部Ｂ２０を有する点でネットワークアクセスゲートウェイＢ１の構成と異なる。

【０１８０】

セッション管理部Ｂ１２は、本実施の第１の実施の形態で説明した機能に加えて、端末Ａ１に対して複数のターゲットＶＬＡＮへのアクセスが許可された場合に、ＩＰアドレス領域重複検出部Ｂ２０に問い合わせて各ターゲットＶＬＡＮに対応するＩＰアドレス領域に重複があるかないかを調べる。重複があった場合、ターゲットＶＬＡＮ内のＤＮＳサーバからのＤＮＳ応答を、重複しないＩＰアドレスに変換して端末Ａ１に転送するよう、ＤＮＳクエリ／応答変換テーブルＢ２１に対して設定する。さらに、ルーティングテーブルＢ１３ａに対しても、ＤＮＳクエリ／応答のＩＰアドレス変換に対応してルーティング処

理部Ｂ１４がＩＰアドレス変換を行うようにエントリを設定する。

【０１８１】

ＩＰアドレス領域重複検出部Ｂ２０は、セッション管理部Ｂ１２からの要求に基づいて、各ターゲットＶＬＡＮに対応するＩＰアドレス領域についてＩＰアドレス領域の重複があるかを調べて応答する。さらに、重複を検出した場合は、各ターゲットＶＬＡＮのＩＰアドレス領域が重複しないためにはどのようにＩＰアドレス変換すべきかを求め、セッション管理部Ｂ１２に対して応答する。

【０１８２】

図１１にＩＰアドレス領域重複検出部Ｂ２０の動作の例を示す。１つ目の例では、セッション管理部Ｂ１２が、ターゲットＶＬＡＮ Ｄ１（ＩＰアドレス領域：１０／８）とターゲットＶＬＡＮ Ｄ２（ＩＰアドレス領域：２０／８）の２つのターゲットＶＬＡＮについてＩＰアドレス領域が重複するかどうかを検出する要求を送った場合、２つのＩＰアドレス領域には重複がないため、ＩＰアドレス領域重複検出部Ｂ２０は、重複なしを応答する。２つ目の例では、セッション管理部Ｂ１２が、ターゲットＶＬＡＮ Ｄ１（ＩＰアドレス領域：１０／８）とターゲットＶＬＡＮ Ｄ３（ＩＰアドレス領域：１０／８）の２つのターゲットＶＬＡＮについてＩＰアドレス領域が重複するかどうかを検出する要求を送った場合、２つのＩＰアドレス領域は重複するため、ＩＰアドレス領域重複検出部Ｂ２０は、ターゲットＶＬＡＮ Ｄ３については、１０／８のＩＰアドレスを３０／８にＩＰアドレス変換すれば重複しないという応答をする。なお、この応答内容はあくまで一例であり、重複しないＩＰアドレス領域を応答するものであれば、どのようなものであっても良い。

【０１８３】

ＤＮＳクエリ／応答転送テーブルＢ２１は、ＤＮＳクエリ転送テーブルＢ１５に設定されるパラメータに加えて、ＤＮＳプロキシ部Ｂ１６がターゲットＶＬＡＮ内のＤＮＳサーバからのＤＮＳ応答を端末Ａ１に転送する際に、応答するＩＰアドレスをどのように変換すべきかというパラメータがエントリとして格納されているテーブルである。図１２にＤＮＳクエリ／応答転送テーブルＢ２１の例を示す。図１２を参照すると、ＩＰアドレス変換が必要なターゲットＶＬＡＮに対するＤＮＳクエリ／応答に関しては、ＤＮＳクエリ／応答転送用のパラメータとして実際のＩＰアドレス領域と変換するＩＰアドレス領域が設定される。ドメインネーム領域がａａａ．ｃｏｍであるターゲットＶＬＡＮに関してはＤＮＳクエリ／応答に対してＩＰアドレス変換を行う必要はないが、ドメインネーム領域がｃｃｃ．ｃｏｍであるターゲットＶＬＡＮに対しては、実際のターゲットＶＬＡＮのＩＰアドレス領域が１０／８であるものを、３０／８のＩＰアドレス領域にＤＮＳプロキシ部Ｂ１６で変換してＬＡＮ内端末にみせる必要があることを示す。この場合のＤＮＳプロキシ部Ｂ１６におけるＤＮＳクエリおよびＤＮＳ応答の変換の例を図１３に示す。ここで、ＤＮＳサーバＧ１は、ドメインネーム領域がｃｃｃ．ｃｏｍであるターゲットＶＬＡＮ内にあるＤＮＳサーバである。

【０１８４】

図１３を参照すると、Ａレコード解決とＰＴＲレコード解決との２種類のＤＮＳメッセージの変換の例が示されている。Ａレコード解決（ドメインネームに対するＩＰアドレスの解決。ＩＰｖ６の場合はＡＡＡＡレコードを解決する。）の場合、ＤＮＳプロキシ部Ｂ１６は、端末Ａ１から受信したＤＮＳクエリについてはそのままターゲットＶＬＡＮ内のＤＮＳサーバＧ１に転送するが、ＤＮＳサーバＧ１から戻されたＤＮＳ応答については、ｗｗｗ．ｃｃｃ．ｃｏｍに対応するＩＰアドレスを１０．２．３．４から３０．２．３．４に変換して端末Ａ１に転送している。また、ＰＴＲレコード解決（ＩＰアドレスに対するドメインネームの解決）の場合、ＤＮＳプロキシ部Ｂ１６は、端末Ａ１から受信したＤＮＳクエリについては、３０．２．３．４を１０．２．３．４に変換してＤＮＳサーバＧ１に転送し、ＤＮＳサーバＧ１から戻されたＤＮＳ応答については、そのまま端末Ａ１に転送している。すなわちターゲットＶＬＡＮ側では実際には１０／８のＩＰアドレス領域が用いられているが、端末Ａ１には上記ターゲットＶＬＡＮ側において、あたかも３０／８

のＩＰアドレス領域が用いられていると見せるようにＤＮＳプロキシ部Ｂ１６によってＤＮＳメッセージのＩＰアドレスを変換する。

【０１８５】

次に、ＤＮＳプロキシ部Ｂ１６が行うＤＮＳクエリ／応答のＩＰアドレス変換に対応して、ルーティング処理部Ｂ１４もＩＰアドレス変換を行うように、セッション管理部Ｂ１２がルーティングテーブルＢ１３ａに対して行う設定について説明する。

【０１８６】

図１２に示したＤＮＳクエリ／応答転送テーブルＢ２１に対応するルーティングテーブルＢ１３ａの例を図１４に示す。図１４を参照すると、第１番目のエントリでは、端末Ａ１から受信したパケット（入力インターフェース：ｅｔｈ１，ソースＩＰアドレス：１９２．１６８．０．５）に対して、１０／８のＩＰアドレス領域に含まれる宛先ＩＰアドレスの場合は、ソースＩＰアドレスを１０．１．１．３に変換してｅｔｈ０：５のインターフェースから出力するのに対し、３０／８のＩＰアドレス領域に含まれる宛先ＩＰアドレスの場合は、ソースＩＰアドレスを１０．１．１．３に変換し、宛先ＩＰアドレスを１０／８のＩＰアドレス領域のＩＰアドレスに変換してから、ｅｔｈ０：６のインターフェースから出力するということを示している。ここで、３０／８の宛先ＩＰアドレスを１０／８のＩＰアドレス領域に変換するというのは、３０．３．４．５を１０．３．４．５に変換するというように、３０／８の領域に含まれるＩＰアドレスを１０／８の領域に含まれるＩＰアドレスに１対１にマッピングすることを示している。

【０１８７】

ルーティングテーブルＢ１３ａの第２番目と第３番目のエントリは、ターゲットＶＬＡＮから受信したパケットに対するルーティング方法が登録されている。第２番目のエントリでは、ｅｔｈ０：５の仮想インターフェースから入力した、ソースＩＰアドレスが１０／８のＩＰアドレス領域に含まれ、宛先ＩＰアドレスが１０．１．１．３であるパケットに対しては、宛先ＩＰアドレスを１９２．１６８．０．５に変換して、ｅｔｈ１のインターフェースから出力するということを示している。第３番目のエントリでは、ｅｔｈ０：６の仮想インターフェースから入力した、ソースＩＰアドレスが１０／８のＩＰアドレス領域に含まれ、宛先ＩＰアドレスが１０．１．１．３であるパケットに対しては、宛先ＩＰアドレスを１９２．１６８．０．５に変換すると共にソースＩＰアドレスを３０／８に変換してｅｔｈ１のインターフェースから出力するということを示している。

【０１８８】

次に、図１５を参照して、本実施の形態において、端末Ａ１がネットワークアクセスゲートウェイＢ３に対して、ＷＡＮ内のターゲットＶＬＡＮへアクセスするための認証要求を出した場合のネットワークアクセスゲートウェイＢ３における動作について詳細に説明する。

【０１８９】

図１５に示すステップＳ２０１～Ｓ２０８の動作はそれぞれ、図５に示した本発明の第１の実施の形態の動作における、ステップＳ１０１～Ｓ１０８に対応する。図１５に示す動作は、ステップＳ２０４でアクセスが許可された各ターゲットＶＬＡＮに対応する仮想インターフェースを作成してからステップＳ２０５でルーティングテーブルエントリの作成を行うまでの動作が異なる。

ステップＳ２０４の後、セッション管理部Ｂ１２は、端末Ａ１に対してアクセスが許可された各ターゲットＶＬＡＮに対するＩＰアドレスをＩＰアドレス領域重複検出部Ｂ２０に渡し、ＩＰアドレス領域重複検出部Ｂ２０はそれぞれのＩＰアドレス領域に重複がないかを調べる（ステップＳ２１０）。ここで、端末Ａ１から新規にアクセスできるように設定しているターゲットＶＬＡＮ間のＩＰアドレス領域重複だけではなく、既に端末Ａ１に対してアクセスが許可されて設定が完了しているターゲットＶＬＡＮとのＩＰアドレス領域重複も調べられる。

【０１９０】

ステップＳ２１０の結果、ＩＰアドレス領域に重複がなければそのままステップＳ２０

５に進む。

【０１９１】

ステップＳ２１０の結果、ＩＰアドレス領域に重複があれば、ＩＰアドレス領域重複検出部Ｂ２０は、各ターゲットＶＬＡＮのＩＰアドレス領域が重複しないためにはどのようにＩＰアドレス変換すべきかを求め、セッション管理部Ｂ１２に対して応答する（ステップＳ２１１）。

【０１９２】

ステップＳ２１１の後、ステップＳ２０５およびＳ２０６で、セッション管理部Ｂ１２はルーティングテーブルＢ１３ａおよびＤＮＳクエリ／応答転送テーブルＢ２１の設定を行うが、ここではステップＳ２１０で求められたＩＰアドレス変換方法がルーティングテーブルＢ１３ａおよびＤＮＳクエリ／応答転送テーブルＢ２１の設定に反映される。

【０１９３】

また、第１の実施の形態では、

１．端末認証部Ｂ１１が端末Ａ１からの認証要求に対して直接認証を行うのではなく、各ターゲットＶＬＡＮに存在する認証サーバＥ１～Ｅ３に対して認証要求を転送し、認証サーバＥ１～Ｅ３が実際の認証を行う形態

２．ネットワークアクセスゲートウェイＢ１が認証ＶＬＡＮスイッチＣ２によってターゲットＶＬＡＮ Ｄ１～Ｄ３と接続されており、端末認証部Ｂ１１が端末Ａ１からの認証要求に対して直接認証を行うのではなく、認証ＶＬＡＮスイッチＣ２に対して認証要求を転送し、認証ＶＬＡＮスイッチＣ２（もしくは認証ＶＬＡＮスイッチに接続されている外部の認証サーバ）が実際の認証を行う形態

３．端末Ａ１から所望のターゲットＶＬＡＮへのアクセスを行うために必要な全ての設定パラメータを、端末認証部Ｂ１１からセッション管理部Ｂ１２へ渡すのではなく、一部の設定パラメータを、ターゲットＶＬＡＮ内の設定サーバからネットワークアクセスゲートウェイ内の設定クライアントが自動的に取得して設定を行う形態

４．ネットワークアクセスゲートウェイＢ１において、ＤＮＳプロトコルにおけるクエリ／応答だけではなく、その他の種類の名前解決プロトコルにおけるクエリ／応答のプロキシ処理が行われる形態

の４つの考えられる他の実施の形態についても併せて説明したが、第２の実施の形態においても、同様の実施の形態をとることが可能である。

【０１９４】

なお、図１０に示したネットワークアクセスゲートウェイＢ３は、コンピュータによって実現可能である。ネットワークアクセスゲートウェイＢ３をコンピュータによって実現する場合には、コンピュータをネットワークアクセスゲートウェイＢ３として機能させるためのプログラムを記録した記録媒体（ディスク、半導体メモリ、その他の記録媒体）を用意しておく。コンピュータは、この記録媒体に記録されたプログラムを読み込み、自身の動作を制御することにより、自コンピュータ上に、端末認証部Ｂ１１、セッション管理部Ｂ１２、ルーティングテーブルＢ１３ａ、ルーティング処理部Ｂ１４、ＤＮＳプロシキ部Ｂ１６、インターフェースドライバＢ１７、ネットワークインターフェースＢ１８、ＩＰアドレス領域重複検出部Ｂ２０、ＤＮＳクエリ応答転送テーブルＢ２１を実現する。

【０１９５】

次に本実施の形態の効果について説明する。

【０１９６】

本実施の形態では、ネットワークアクセスゲートウェイＢ１は、ＬＡＮ内の端末Ａ１からの認証要求に基づいて端末Ａ１が所望するターゲットＶＬＡＮへのアクセスが可能になるように設定を行う際に、端末Ａ１に対してアクセスが許可されたターゲットＶＬＡＮ間にＩＰアドレス領域の重複がないかどうかを検出し、重複があった場合は、互いに重複しないＩＰアドレス領域にＩＰアドレス変換すべく、ルーティングテーブルＢ１３のエントリ、ＤＮＳクエリ／応答転送テーブルＢ２１のエントリの設定を行う。

【０１９７】

従来技術では、ネットワークアクセスゲートウェイは、ＬＡＮ内端末を互いにＩＰアドレス領域が重複するターゲットＶＬＡＮにアクセスさせることはできなかったが、本実施の形態により、端末の送受信するパケットおよびＤＮＳクエリ／応答を互いに重複しないＩＰアドレス領域に変換することで、上記端末にはあたかも互いに重複しないＩＰアドレス領域をもつターゲットＶＬＡＮにアクセスしているように見せることが可能になり、端末をＩＰアドレス領域の重複する複数のターゲットＶＬＡＮにアクセスさせることが可能となる。

【図面の簡単な説明】

【０１９８】

【図１】本発明の第１の実施の形態の構成を示すブロック図である。

【図２】本発明の第１の実施の形態のルーティングテーブルの例を示す図である。

【図３】本発明の第１の実施の形態のＤＮＳクエリ転送テーブルの例を示す図である。

【図４】本発明の第１の実施の形態のインターフェースドライバにおけるインターフェース設定テーブル例を示す図である。

【図５】本発明の第１の実施の形態のネットワークアクセスゲートウェイの動作を示すフローチャートである。

【図６】本発明の第１の実施の形態から考えられる１つ目の他の実施の形態の構成を示すブロック図である。

【図７】本発明の第１の実施の形態から考えられる２つ目の他の実施の形態の構成を示すブロック図である。

【図８】本発明の第１の実施の形態から考えられる３つ目の他の実施の形態の構成を示すブロック図である。

【図９】本発明の第１の実施の形態から考えられる３つ目の他の実施の形態のネットワークアクセスゲートウェイの動作を示すフローチャートである。

【図１０】本発明の第２の実施の形態の構成を示すブロック図である。

【図１１】本発明の第２の実施の形態のＩＰアドレス領域重複検出部の動作例を示すフローチャートである。

【図１２】本発明の第２の実施の形態のＤＮＳクエリ／応答転送テーブルの例を示す図である。

【図１３】本発明の第２の実施の形態のＤＮＳプロキシ部の動作例を示すフローチャートである。

【図１４】本発明の第２の実施の形態のルーティングテーブルの例を示す図である。

【図１５】本発明の第２の実施の形態のネットワークアクセスゲートウェイの動作を示すフローチャートである。

【符号の説明】

【０１９９】

Ａ１…端末

Ｂ１～Ｂ３…ネットワークアクセスゲートウェイ

Ｂ１１…端末認証部

Ｂ１２…セッション管理部

Ｂ１３、Ｂ１３ａ…ルーティングテーブル

Ｂ１４…ルーティング処理部

Ｂ１５…ＤＮＳクエリ転送テーブル

Ｂ１６…ＤＮＳプロキシ部

Ｂ１７…インターフェースドライバ

Ｂ１８…ネットワークインターフェース

Ｂ１９…ＤＨＣＰクライアント

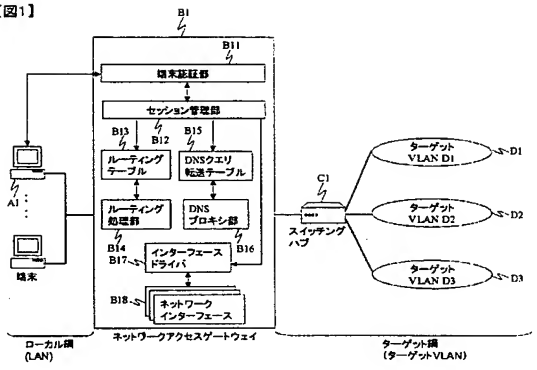
Ｂ２０…ＩＰアドレス領域重複検出部

Ｂ２１…ＤＮＳクエリ／応答転送テーブル

Ｃ１…スイッチングハブ

Ｃ２…認証ＶＬＡＮスイッチ
Ｄ１～Ｄ３…ターゲットＶＬＡＮ
Ｅ１～Ｅ３…認証サーバ
Ｆ１～Ｆ３…ＤＨＣＰサーバ
Ｇ１…ＤＮＳサーバ
１０３　インターフェース設定テーブル

【図１】
【図1】



【図２】
【図2】

B13 ルーティングテーブル

入力			出力			
入力インターフェース	ソースIPアドレス	宛先IPアドレス	ソースIPアドレス	宛先IPアドレス	ゲートウェイIPアドレス	出力インターフェース
eth1	192.168.0.2	10/8	10.1.1.1	—	10.1.1.254	eth0:0
		20/8	20.1.1.1	—	20.1.1.254	eth0:1
	192.168.0.3	20/8	20.1.1.2	—	20.1.1.254	eth0:2
		10/8	10.1.1.2	—	10.1.1.254	eth0:3
	192.168.0.4	10/8	10.1.1.2	—	10.1.1.254	eth0:4
eth0:0	10/8	10.1.1.1	—	192.168.0.2	—	eth1
eth0:1	20/8	20.1.1.1	—	192.168.0.2	—	eth1
eth0:2	20/8	20.1.1.2	—	192.168.0.3	—	eth1
eth0:3	10/8	10.1.1.2	—	192.168.0.3	—	eth1
eth0:4	10/8	10.1.1.2	—	192.168.0.4	—	eth1

【図３】
【図3】

B15 DNSクエリ転送テーブル

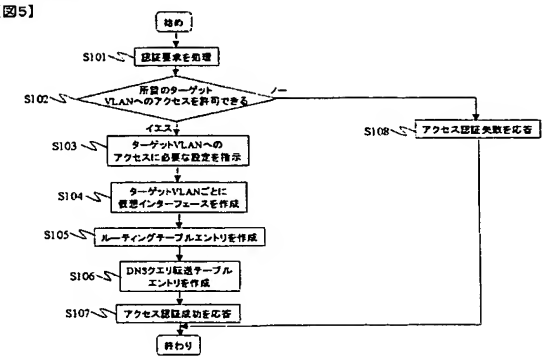
入力			出力		
入力インターフェース	ソースIPアドレス	入力クエリ	ソースIPアドレス	DNSサーバ	出力インターフェース
eth1	192.168.0.2	*.aaa.com, 10/8	10.1.1.1	10.1.2.3	eth0:0
		*.bbb.com, 20/8	20.1.1.1	20.1.2.3	eth0:1
	192.168.0.3	*.bbb.com, 20/8	20.1.1.2	20.1.2.3	eth0:2
		*.ccc.com, 10/8	10.1.1.2	10.1.3.4	eth0:3
	192.168.0.4	*.aaa.com, 10/8	10.1.1.2	10.1.2.3	eth0:4

【図４】
【図4】

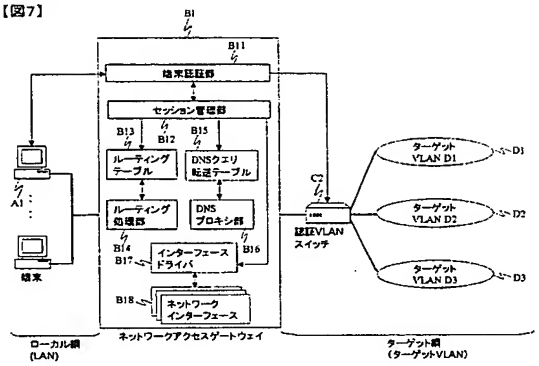
103 インターフェイス設定テーブル

物理インターフェース	仮想インターフェース	MACアドレス	VLANタグID	IPアドレス	ネットマスク
eth0	eth0:0	0:0:0:0:0:1	100	10.1.1.1	255.255.255.0
	eth0:1	0:0:0:0:0:2	200	20.1.1.1	255.255.255.0
	eth0:2	0:0:0:0:0:3	200	20.1.1.2	255.255.255.0
	eth0:3	0:0:0:0:0:4	300	10.1.1.1	255.255.255.0
	eth0:4	0:0:0:0:0:5	100	10.1.1.2	255.255.255.0
eth1	なし	1:2:3:4:5:6	なし	192.168.0.254	255.255.255.0
…	…	…	…	…	…

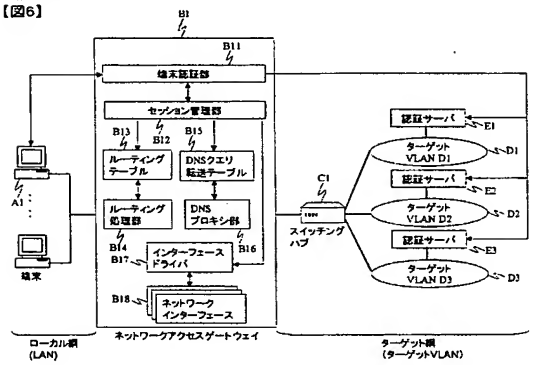
【図５】
【図5】



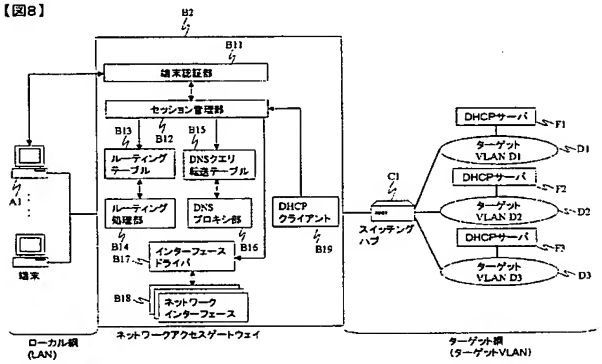
【図７】
【図7】



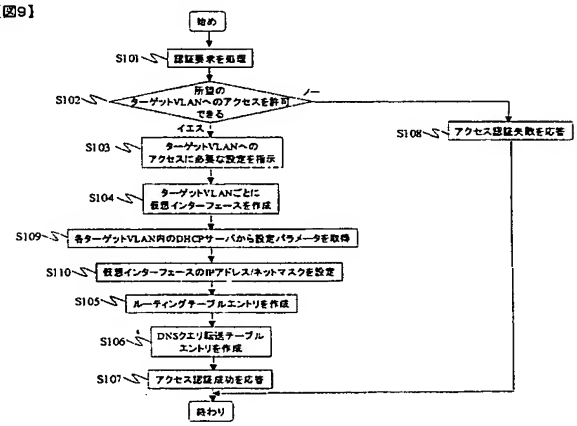
【図６】
【図6】



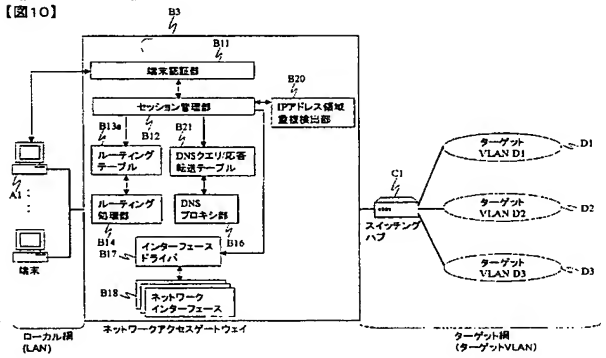
【図８】
【図8】



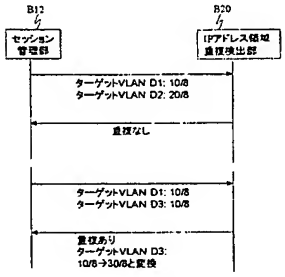
【図９】
【図9】



【図１０】
【図10】



【図１１】
【図11】

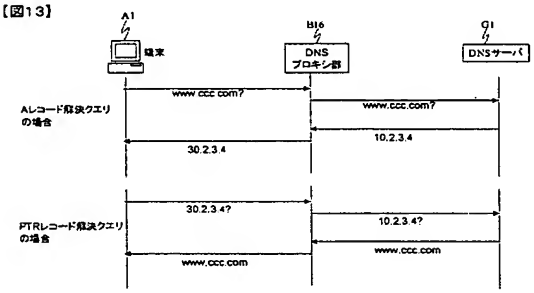


【図１２】
【図12】

B21 DNSクエリ／応答転送テーブル

入力			出力			IPアドレス変換	
入力インターフェース	ソースIPアドレス	入力クエリ	ソースIPアドレス	DNSサーバ	出力インターフェース	変換前IPアドレス領域	変換後IPアドレス領域
eth1	192.168.0.5	*.aaa.com, 10/8	10.1.1.3	10.1.2.3	eth0:5	--	--
		*.ccc.com, 30/8	10.1.1.3	10.1.3.4	eth0:6	10/8	30/8

【図１３】
【図13】

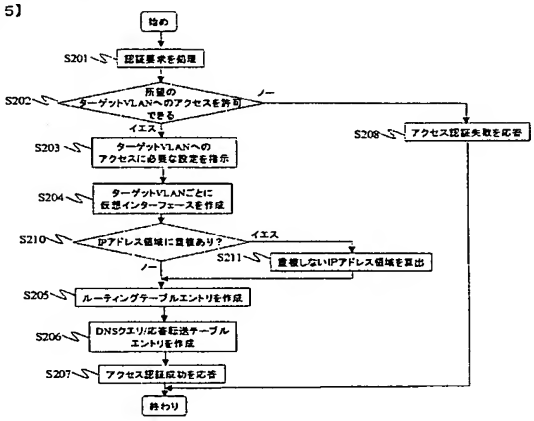


【図１４】
【図14】

B13a ルーティングテーブル

入力			出力			
入力インターフェース	ソースIPアドレス	宛先IPアドレス	ソースIPアドレス	宛先IPアドレス	ゲートウェイIPアドレス	出力インターフェース
eth1	192.168.0.5	10/8	10.1.1.3	—	10.1.1.254	eth0:5
		30/8	10.1.1.3	10/8	10.1.1.254	eth0:6
eth0:5	10/8	10.1.1.3	—	192.168.0.5	—	eth1
eth0:6	10/8	10.1.1.3	30/8	192.168.0.5	—	eth1

【図１５】
【図15】



フロントページの続き

Fターム(参考) 5K030 HA08 HD03 HD06 HD09 KA01 KA05 LB01 LB06
5K033 CB09 CC01 DA06 DB12 DB18 EC04